MINISTRY OF EDUCATION OF THE REPUBLIC OF BELARUS
Belarusian National Technical University

Faculty of Management Technologies and Humanitarization
Department of "Philosophical Teachings"

A.I. Loiko

CYBER SECURITY PHILOSOPHY AND METHODOLOGY

Textbook on general education discipline "Philosophy and Methodology of Science" for students all forms of education

Electronic learning material

Minsk
BNTU
2023

Author:

A.I. Loiko Sciences, Professor, Head of the Department "Philosophical Teachings" of the Belarusian National Technical University

Reviewers:

Kandrichina I.N., Associate Professor, Department of Management, Belarusian National Technical University, Candidate of Sociological Sciences

Nekrashevich F.A., Associate Professor of the Department of Philosophy and Ideological Work of the Educational Institution "Academy of the Ministry of Internal Affairs of the Republic of Belarus" Candidate of Historical Sciences

The textbook complements the lecture material with topical issues of cyber security philosophy and methodology. This applied material is important for specialists in management, marketing, logistics and engineering and economic specialties.

CONTENTS

INTRODUCTION

The concept of security is widely used in various fields of professional activity, as well as at the level of forming state development strategies, assessing the international situation and personal security. Since we are talking about a systemic phenomenon, we distinguish such conceptual levels of its understanding as particular theories of security, general theory of security and philosophy of security.

At the level of practical activities of the state, a special topic is the issues of ensuring demographic, information, food, energy, industrial, military-political, intellectual security and law and order. At the level of corporate structures, issues of information and technological security play an important role. At the personal level, the concepts of legal security play an important role.

Ensuring security involves not only the human factor and the institutional environment, but also the technological provision of activity systems with devices and security software products. The concept of danger plays an important role when considering the concept of safety. This concept has objective grounds related to the characteristics of natural and technical systems, as well as the human factor in the form of elementary non-compliance with technological discipline and labor protection.

Objective components of natural and technological hazards have updated the idea of risks and threats. These ideas are formalized by the mathematical apparatus of probability theory, catastrophe theory and risk theory.

Along with natural disasters, the modern period of human development is characterized by a whole set of cataclysms, threats and dangers that are social in nature and have a qualitatively different nature. These threats and dangers are inherent at both the global, regional and local levels. This is the problem of new poverty, the threat of a population explosion, environmental dangers, aggressive ethnic nationalism and separatism.

SECURITY PHILOSOPHY

The philosophy of security focuses on the peculiarities of the functioning of 1) natural systems within the framework of the concepts of their linear and nonlinear development, which are formulated by the ontology and philosophy of nature; 2) technical and technological complexes (philosophy of technology); 3) individual and social consciousness of people (philosophy of consciousness); 4) social information systems (philosophy of information); 5) institutional corporate structures (management philosophy).

The vector of philosophical knowledge moves to phenomena related to preventing threats to everyday life and ensuring personal and social security. The need for security is one of the anthropological constants of human existence. She accompanies man throughout history. Providing security is a social experience that is one of the most important for a person. The ability to prevent threats and formulate a security strategy serves as an indicator of the sociocultural development of society. Ideas about security reflect complex processes in the structure of archetypes. The level of safety is a specific indicator of the state of society; ideas about what is dangerous and what is safe reflect the self-awareness of society and the dominant value orientations in it.

The substantive characteristic of safety is activity. Security is a specific set of operating conditions. That is why they talk about safe operating conditions, about finding someone or something in safe conditions. It is necessary to distinguish objectively safe, favorable conditions from the subject’s subjective idea of the totality of conditions under his control, which in reality are not such. The description of security as a state of protecting someone or something from a set of threats is an expression of subjective, everyday, everyday ideas about security. Ensuring security is the process of creating favorable conditions for activity, the process of a subject mastering the necessary conditions for his own existence. Ensuring the security of a subject is the creation of conditions under which his interests would be realized, the goals set by him, based on his values, would be realized. This means that security is the conditions in which subjects preserve and reproduce their values.

Ensuring security as a process of mastering the conditions of existence is at the same time a process of realizing the freedom of the subject as the ability to control the conditions of one's own existence. Freedom and security are closely interrelated phenomena that form fundamental aspects of social existence, the most important characteristics of social subjects.

SECURITY ONTOLOGY AND PHILOSOPHY OF NATURE

Any person, thinking about security, inevitably brings into the field of view of his thinking the concepts of danger, risks and threats. He also encounters the concept of "source of dangers, risks and threats." Ontology and philosophy of nature study the objective sources of danger, risks and threats to humanity and the individual. In this context of research, it has been stated that the objective source of danger, risks and threats is the dynamics of natural systems. Most sources of danger and risks for humanity are found in inanimate nature systems. Less in systems of biological nature, since one of the conditions for their existence and evolution in the local spaces of planets is the presence of the resource of adaptation to these spaces. Self-organization plays a key role in the creation of ecosystems and their dynamic equilibrium. This can be seen in the example of the Earth's biosphere.

Ancient philosophers understood that even small changes that disrupt harmony can significantly change the world and plunge it into chaos. For many centuries, their attention was occupied precisely by the laws of this harmony, for in it they saw a manifestation of the divine will that keeps the world in order. Starting with the Pythagoreans, who discovered that these laws can be written in the language of numbers and geometric figures, mathematics began to be used as a means of reflecting the ideal laws of nature, in which all opposites are proportionate and balanced. Perhaps this explains the stubborn reluctance of "classical” mathematicians to consider unstable mathematical models in which a sharp imbalance is possible.

Only in the twentieth century did works appear that seriously suggested that such instabilities are as real as states of harmony. It was realized that any system, as it develops, goes through stages of restructuring, abrupt change, during which a regrouping of forces and a reorganization of balance occurs. These stages are characterized by a temporary predominance of one of the forces, which leads to chaos that destroys previous structures; then harmonization occurs, balance is restored, but in a new, qualitatively different state.

One of the mathematical theories that describes abrupt transitions is the theory of catastrophes. As a scientific discipline, it appeared in the 70s of the twentieth century. The advantage of this theory is that it does not require detailed mathematical models and can describe situations not quantitatively, but qualitatively, and its results and conclusions are illustrated by simple geometric images. The theory of catastrophes explains many phenomena at a qualitative level. It, along with other modern theories of dynamic systems, changed the usual ideas about the stability and inertia of the physical world.

Since in certain situations - at points of catastrophe - even minor movements can affect the course of development, the ability to determine how far the system is from such a point will be very useful. Formally, to do this, one should study the dependence of the system on external parameters in mathematical models. However, in practice there are often cases when the researcher does not even have vague ideas about what evolutionary equation describes the development of the system. Even in these situations, pathological from the point of view of mathematical modeling, it is possible to indicate some indirect signs that the system being studied is near the point of disaster.

We are talking about the so-called “catastrophe flags” - features of the behavior of the system, by which one can judge the approach of a critical point. This is the presence of several different stable states; the existence of unstable states from which the system is removed by weak “pushes”; the ability to quickly change the system with small changes in external conditions; irreversibility of the system (impossibility of returning to previous conditions); hysteresis.

The theory of catastrophes is one of the parts of a more general mathematical theory - the qualitative theory of complex nonlinear systems. This theory studies the general principles that appear in different situations and helps to better understand the mechanism of natural forces. The differences between linear and nonlinear systems are of interest. The linear view in physics generally expresses the principle of superposition - the force acting on an element will be equal to the sum of the acting forces. From a mathematical point of view, a relationship will be linear when the number of changes in one independent quantity corresponds to the same number of changes in another dependent on it.

A system that obeys linear laws is a system equal to the sum of its parts. Knowing such patterns of elements and systems, it is easy to predict behavior and design objects. A linear view of the world is easy to understand, logical, and common sense. They tried to transfer it from mechanistic systems to the entire surrounding world. But linear processes turn out to be rather an exception, since natural phenomena are much more complex. Nonlinear relationships in different natural phenomena and sciences are described by similar models, predicting the same final results. A linear description turns out to be only a special case of nonlinear processes.

Nonlinearity describes fundamental and universal connections and relationships between objects. It can be called the opposite of linearity. Nonlinearity negates the principle of superposition and offers nothing in return.

In nonlinear systems, qualitatively different properties appear that are not present in the parts that make up the system. It is necessary to distinguish between a random process and deterministic chaos.

Self-organization is the emergence of order from chaos. This process, often referred to in organizational management, is also observed in nonliving, living, and social systems.

Maintaining order requires energy that comes into an open system from the outside. After this, the energy dissipates.

In conditions of disorder, order changes randomly. Some changes increase rapidly and drain energy from the rest of the system through nonlinear interactions. Growing changes subjugate the energetically weak ones. An ordered coherent structure of the system is formed. There is a nonlinear relationship between the force of impact and the reaction of a dissipative system. Despite great efforts, the result may be insignificant. On the other hand, a weak signal under certain conditions can accelerate, and a swinging process will arise.

Such phenomena are possible due to positive reinforcing and negative counteracting feedback connections. The structure of the system is a set of feedbacks and relationships between them. Therefore, imposing a certain development plan on a nonlinear system can lead to unpredictable results.

As soon as a system is described by the simplest nonlinear mathematical equation, it immediately has alternative evolutionary paths.

A nonlinear system does not change qualitatively for a certain time. But when a threshold value is reached, a crisis situation occurs when complex open systems are characterized by unstable behavior. At such critical moments, even small changes can change the trajectory of development.

Bifurcation is understood as the choice of a qualitatively different development path, which is random. Two identical complex systems will differ over time. Because the systems find themselves in different, even slightly different, conditions. At the same time, the system has only a limited number of alternative development paths. The range of possible evolutionary paths is determined by the properties of the system.

FUNDAMENTAL PROPERTIES OF COSMIC NATURAL SYSTEMS: CATASTROPHISM

In understanding natural systems, two conceptual approaches are justified. One of them is designated as catastrophism. He points out that any natural system contains danger and risks for humanity. Similar dangers and risks are demonstrated by the topic of the Universe associated with the discussion of its formation and subsequent dynamics. The Big Bang is considered the starting point of the history of the Universe.

The Big Bang theory is a cosmological model that describes the early stages of the development of the Universe. At the beginning of the 20th century, astronomers discovered that galaxies were flying apart in different directions. It follows from this that the Universe is expanding. The moment from which the expansion of the Universe began is called the “Big Bang”. This happened 13.8 billion years ago.

The Big Bang theory describes the early stages of the expansion of the Universe. Events that took place immediately after the Big Bang. The processes after the Big Bang were due to the fact that the Universe gradually cooled and became less dense. As we know, temperature is a measure of the movement of particles. The slower the particles move, the easier it is for them to connect with each other. As the Universe cooled, at first, separately flying quarks were able to combine into protons, neutrons and other hadrons and leptons.

Then the already obtained particles, continuing to slow down, began to form the first nuclei of atoms.

The period of formation of the first atoms in the Universe is called primary nucleosynthesis. It lasted approximately 20 minutes after the Big Bang. During this period, the Universe was heated to a state like inside stars. During this period, the nuclei of hydrogen and helium were mainly formed in a ratio of 3 to 1. Such proportions of hydrogen and helium, the two most common elements in the Universe, are still observed today.

After the primary nucleosynthesis ended, and almost no new atomic nuclei were formed, the Universe still remained so hot that the matter in it was in a plasma state. In it, electrons flew separately from nuclei. Thanks to free-flying electrons, the Universe was opaque to light during this period. Photons constantly collided with electrons and could not fly straight, as if they were locked in a mirror maze.

The universe continued to cool, and about 300,000 years after the Big Bang, the temperature had cooled enough for electrons to attach to the nuclei of atoms, and as a result, the universe became transparent. This moment is called recombination. The photons that filled everything around no longer saw obstacles in the form of electrons and were able to fly directly from everywhere and in all directions at once.

The photons that were released at the moment of recombination are still visible today. After 13 billion years, they arrive in the form of cosmic microwave background radiation.

The discovery of cosmic microwave background radiation is one of the main confirmations of the Big Bang Theory. Its important feature is homogeneity. On large scales, the Universe is the same in all directions.

There are inaccuracies in the theory itself that will need to be eliminated by further more accurate and detailed astronomical observations and the development of more advanced physical models. But the amount of independent cross-sectional data that modern cosmology already has allows us to say with confidence that the Big Bang, which became the starting point for the expansion of the Universe, really happened.

According to new research, some of the most powerful space disasters and explosions ever observed by astronomers are driven by massive space objects with incredibly strong magnetic fields. Gamma-Ray Bursts (GRBs) are intense bursts of high-energy X-ray radiation recorded by astronomers in various parts of the Universe. They are the most powerful high-energy events, releasing energy equivalent to the energy emitted by the Sun in 10 billion years into space in a short time, from milliseconds to a few seconds.

Scientists suspect that gamma-ray explosions may be caused by two different energy sources. Considering the data obtained from recording the longest and most intense gamma-ray explosion, scientists found that the cause of this event could be a third source, an object made of magnetic material, the size of which is only a few tens of kilometers, but a magnetic field that is stronger than the magnetic field the Earth's field is at least 5000 trillion times.

Gamma explosions are divided into two groups according to their duration, short and long, respectively. The separation threshold is a time of 2 seconds. Brief explosions usually occur when two or more neutron stars, remnants of ordinary stars with incredibly dense matter and a strong magnetic field, merge. Longer gamma-ray bursts are usually associated with supernova explosions. Scientists have suggested the existence of another type of gamma explosions - ultra-long-lasting, such explosions last more than 10 thousand seconds (2 hours 46 minutes and 40 seconds). After analyzing all available data, scientists discovered four such events and tried to find out the cause of their occurrence, the source of their energy and other parameters.

An in-depth analysis of data from the gamma-ray explosion GRB 111209A, recorded by the Swift spacecraft in 2011, provided some clues to scientists. This explosion is the brightest and longest lasting of all gamma-ray explosions recorded, lasting 15,400 seconds and the energy of the explosion was equivalent to 500 times the energy emitted by the Sun during its entire life cycle.

Since even the afterglow from the gamma explosion of GRB 111209A has now ceased, scientists made observations of this part of space using the GROND instrument mounted on the 2.2-meter MPG/ESO telescope and the X-shooter instrument of the Very Large Telescope, which are part of European Southern Observatory. These observations provided a very clear signature of the presence of a supernova, which was named SN 2011kl, and this marks the first time in the history of astronomy that a supernova explosion has been directly associated with an ultra-long-lasting gamma explosion. The supernova explosion occurred approximately 6.3 billion years ago at a distance of 13 billion light years from Earth and was caused by the "death" of a star whose mass exceeded the mass of the Sun by 8 to 25 times.

Previously, astronomers had assumed that supernovae, which produce long-lasting gamma-ray bursts, eventually turn into black holes. However, the spectrum of light emitted by supernova SN 2011kl is as close as possible to the emission spectrum of one of the radioactive isotopes of nickel. In addition, the intensity of the glow of SN 2011kl is at least three times higher than the intensity of the glow of supernova remnants associated with long gamma-ray explosions. The source of the ultra-long gamma-ray burst is a magnetar. It is a rapidly rotating neutron star with a strong magnetic field that is at least 5,000 trillion times stronger than the Earth's magnetic field. Further observations of the explosion area of GRB 111209A and other ultra-long gamma-ray explosions will allow scientists after some time to either confirm this theory or refute it by putting forward a new, more realistic theory about the origin of such explosions.

The heat death of the Universe is a conceptual idea in cosmology put forward by Rudolf Clausius in 1865, which proposes that over time the Universe will tend to a state of maximum entropy of uniformity. In this state, all the energy and matter in the Universe will be evenly distributed and isolated. Thus, all processes and forms of life will become impossible.

If the Universe is flat or open, then it will expand forever and as a result of such evolution it is expected that it will reach a state of thermal death, that is, as the Universe expands, matter will move further and further away from each other under the influence of Dark Energy. Stars will eventually burn out, black holes will evaporate thanks to Hawking Radiation, and particles will disintegrate. There will be nothing left but infinitely expanding space, infinite time and quantum fluctuations.

From the idea of the Heat Death of the Universe follows the idea that in infinite space, with an infinite amount of time, anything can happen. Including the emergence of a Universe exactly the same as today. This idea also follows from quantum mechanics. Empty space is not completely empty; there are quantum fields, the value of which always fluctuates a little at any point in space. The jitters are called "Quantum Fluctuations".

With an infinite amount of time and space, sooner or later a state of minimal entropy (or minimal order) will arise again, which can serve as the basis for the emergence of a separate galaxy, or a new Universe. Also, in such a model of the Universe, there is a high probability of the appearance of simply a separate brain in space; this hypothetical phenomenon is called the “Boltzmann brain”.

The theory of the heat death of the Universe is not without controversy, and it also has its critics. Some of the major controversies and criticisms associated with this theory include: Information Paradox: In the heat death theory of the universe, it is assumed that the entropy of the universe will tend to a maximum and this will lead to a loss of information. However, according to the principle of conservation of information in physics, information cannot be destroyed or lost forever. This paradox raises the question of how information would be preserved or restored in the supposed heat death of the Universe.

The theory of the heat death of the Universe is based on existing physics. But in the future, new physical processes or laws may be discovered that may change the idea of the ultimate fate of the Universe.

Although the heat death of the Universe is one possible scenario, there are other hypotheses and models that predict different ultimate fates of the Universe. Some of these include "Big Rip" scenarios or the possibility of cyclical universes. Critics of the heat death of the Universe call attention to the need to consider and analyze these alternative models.

DYNAMICS OF WILDLIFE ECOSYSTEMS IN THE CATEGORIES OF CATASTROPHISM AND EVOLUTIONISM

All natural ecosystems were formed naturally, without the influence of any anthropogenic factors. They are characterized by the interconnectedness of all components (climate, inorganic substances and organic compounds, plants and animals), between which the exchange of matter and energy occurs. Among the diversity of existing natural ecosystems, there are 3 main groups: terrestrial, marine and freshwater.

In modern biological science, Jean Baptiste Lamarck is considered the founder of the evolutionary approach, although many of his assumptions have not been confirmed. In particular, it turned out that traits acquired as a result of exposure to the external environment are not inherited. Evolutionary theory, as a theory of gradual transformation of animal and plant species, was consistently developed by Charles Robert Darwin. He presented the results of his scientific research in the book: “The Origin of Species by Means of Natural Selection” (1859). He considered the mechanism of evolution to be natural selection in the struggle for existence, during which any changes favorable for survival in given conditions (limited space, food, heat and light) increase the ability to reproduce.

The struggle for existence can be interspecific, intraspecific, and a struggle against unfavorable environmental conditions. The most acute is the intraspecific struggle, since individuals of a given species have the same needs. In the process of natural selection, selective destruction of some individuals and reproduction of others occurs, and useful traits acquired during evolution are inherited. The heredity factor ensures the stability of the species. The direction of natural selection can change when external conditions change, when some other characteristics turn out to be most important for survival. The factor of variability comes into play, determining the emergence of new species.

Evolution, according to Darwin, is a slow process, because nature does not tolerate leaps. However, slow evolution does not explain a number of features associated with the distribution of species on Earth. Modern scientific ideas about the development of living organisms are somewhat different from the ideas of Charles Darwin. So, in the 20th century.

The role of DNA in the transmission of hereditary information was established, and the theory of natural selection was supplemented by mutation theories. Scientists have concluded that mutations arise spontaneously in genes, the environment encourages successful mutations, and as a result of such selection, evolution occurs. Ultimately, evolution is the result of a series of mutations, the carriers of which either survive or die.

The theory of evolution includes data from genetics, paleontology, ecology, molecular biology and the concept of Darwinism, which is why it is called the “synthetic theory of evolution.” Strict laws of evolution have not yet been formulated. Scientists operate with hypotheses that have particular practical confirmation. The synthetic theory of evolution is usually divided into two structural parts: the theory of microevolution and the theory of macroevolution. Within the framework of the theory of microevolution, irreversible transformations of populations are studied, leading to the formation of a new species.

A population is a collection of organisms (individuals) of the same species with a single gene pool, occupying a certain territory. All living things exist in populations. Each population has quantitative boundaries: the minimum number required for reproduction and the maximum achievable maximum number. A species is a group of interbreeding organisms that cannot interbreed with members of other such groups. A species is formed only within one population. In reality, a species exists in the form of populations. The theory of macroevolution studies the origin of supraspecific taxa, as well as the directions and patterns of development of life on Earth in general, including the origin of humans.

The term "taxon" defines the general name of groups of organisms. The universal classification of life forms includes the following taxa: species, genus, family, order (order in plants), class, phylum (division in plants) and kingdom.

The species has the least degree, the kingdom the highest. In the theory of microevolution, the population is considered the elementary evolutionary structure. N.V. Timofeev-Resovsky showed that the emergence of evolutionary phenomena requires the action of the following factors: mutations, fluctuations in the number of individuals, isolation of populations and natural selection. Gene changes - mutations - only supply elementary evolutionary material, but do not in themselves ensure evolution.

The properties acquired as a result of mutation can be destructive for all individuals and for the population as a whole. The evolutionary role of population fluctuations manifests itself in two directions. First, a decrease in numbers leads to an increase in inbreeding. Secondly, a decrease in genotype diversity affects the direction of selection. Fluctuations in numbers can occur in different directions and do not determine the course of hereditary transformations. Isolation of populations disrupts free crossing and perpetuates the resulting differences in the sets and numbers of genotypes in the population. Isolation has both territorial-geographical and biological reasons, for example, preference for feeding sites, differences in reproductive timing.

The role of natural selection in evolution is manifested at the level of the phenotype as a whole, and not at a separate phenotypic trait. Its genetic meaning is the preservation of certain genotypes within a population and their selective participation in the transmission of genes to subsequent generations. Natural selection can manifest itself in two forms: driving selection and stabilizing selection. Driving natural selection gives direction, determines a unique vector of the population, and creates new genotypes. Stabilizing natural selection improves the processes of individual development of individuals without changing the genotype, as a result of which the phenotype prevailing in given conditions is determined. In general, the modern theory of evolution satisfactorily explains the development of life on Earth.

However, many life processes on our planet are catastrophic in nature and do not fit into the pattern of gradual changes. Firstly, the theory of evolution cannot fully explain the phenomenon of the origin of life. Thus, the primary form of life - bacteria - has two thousand enzymes, or enzyme catalysts. It is estimated that, by coincidence, it may take from 40 to 100 billion years for the isolation of these enzymes from the “primordial soup”. However, the Earth has existed for 4.6 billion years. Consequently, life arose on our planet historically suddenly.

Secondly, the evolution of a living being occurs in a coordinated change of many of its elements, which evolve simultaneously. Thirdly, evolution, while affecting individual species and ecological niches, does not at the same time affect other species and niches. For example, sharks have not changed at all over the past 165 million years. About 3 million years ago in Africa, in the zone of the East African Rift, catastrophic processes of geological activity occurred, and local zones of long-term exposure to the flora and fauna of radon, a radioactive gas of magmatic origin, arose there. The high radioactive background of these places greatly enhanced mutational changes, which accelerated the development of East African primates and, ultimately, led to the emergence of humans.

Natural selection acts on living beings integrally and in combination. It simultaneously affects their body, development and behavior. But, probably, another force of evolution reveals itself in development - self-organization. Self-organization is a fundamental concept of synergetics, meaning ordering, i.e. transition from chaos to a structured state, occurring spontaneously in open nonlinear systems. Openness is a property of systems, manifested in their ability to exchange matter, energy and information with the environment, and nonlinearity implies a lot of variability in evolutionary paths.

Self-organization means that any life processes occur not due to internal influence, but due to internal changes in the system itself. Self-organization can provoke optimal changes, but it can also lead the population to death. 30–35 thousand years ago, the ancestors of modern Europeans, having improved hunting tools, began to kill so many animals that many of their species simply disappeared. About 10 thousand years ago, the ancestors of Native Americans hunted mammoths and destroyed them completely.

Over subsequent periods of social development, people moved from hunting to agriculture, mastered crafts, organized trade, began to engage in intellectual activity, and created cities. Currently, there are about 50 million species of animals and plants on our planet. However, since the appearance of life on Earth, the animal and plant worlds have had approximately 50 billion species. It follows that of all the species that have ever existed, only one in a thousand has survived, i.e. to date, 99.9% of the species have died. At the same time, extermination associated with the emergence of humanity amounted to only 5%; the remaining species of living organisms died on their own.

The optimal lifespan of an individual species is 4 million years, while for mammals it is only 1 million years. Over the course of several million years, each species forms, multiplies and prospers, and then dies out. On average, over the entire history of life on the planet, one species died per day. What leads species to extinction with a regularity of 4 million years? The main factor in this process is the geological activity of the Earth.

Thus, over the past 50 thousand years, tropical forests have declined sharply. As a result, diversity in the equatorial rain forests gradually decreased, and unique flora and fauna began to disappear. 10 thousand years ago, glaciers reached the territory of what is now New York, and now they have retreated far to the north. Species live, evolve, and disappear in highly variable environments. This apparently explains 90% of all cases of their extinction.

But with large animals (for example, dinosaurs) the situation is much more complicated. It is possible that these animals are dying out not because of their inability to adapt to changed living conditions, but because of their own behavior. Not only the environment, but also complex living beings themselves are capable of changing and not always for the better. In some cases, their behavior can change the environment so quickly that it drives these animals to extinction. In other cases, animals stop adapting to changes in the environment and also quickly die.

The ideas of Jean Baptiste Lamarck and Charles Darwin about the continuous evolutionary development of living nature are opposed by the theory of catastrophes put forward by Georges Cuvier (1769–1832). While excavating in the Alps, he found that the remains of animals from past eras are not similar to those of today. The bones of ichthyosaurs and plesiosaurs are found in ancient layers, so it is useless to look for them in later deposits, and the bones of manatees and seals should not be looked for next to the remains of ichthyosaurs. In his treatise "Discourses on revolutions on the surface of the globe" (1812), the French paleontologist suggested that not only various catastrophes that moved the layers of our planet gradually pushed various parts of the continents out of the depths of the sea and reduced the basins of the seas, but also the pools themselves moved from one place to another.

Cuvier did a lot in the field of animal semantics, comparative anatomy and paleontology. He belongs to the principle of "correlation of parts of the body," according to which the structure of any organ naturally correlates with the structure of all other organs and the body as a whole. Guided by this principle and having any part of the animal available, the scientist recreated the appearance of the entire living creature. While studying fossil animals, Cuvier established a connection between their structure and paleontological periods.

He noticed that during the transition from ancient to later geological strata, the structure of fossil animals becomes more complex. The natural scientist associated these complications with catastrophic changes in the environment. Since among the marine formations there are layers filled with the remains of land and freshwater animals and plants, he reasoned, parts of the land were periodically flooded. The ruptures and fractures observed in the most ancient layers of the Earth indicate the action of sudden and grandiose natural phenomena. Referring to the absence of transitional forms of living beings, Cuvier came to the conclusion that biological species themselves are unchanged, and extinct species were as constant as modern ones. In 1786, he was the first to announce the extinction of species. Georges Cuvier considered sea floods to be the root cause of global extinctions, but this hypothesis was not confirmed by modern biologists and geologists.

The ocean is advancing slowly, winning a millimeter a year from the land. The flora and fauna have time to adapt to this pace, and rapid mass extinction does not occur. Local floods, rapid inundations of land, have occurred many times in the past, but over a very limited area. They never covered the entire planet and did not cause much damage to land dwellers. The largest flood occurred 6 million years ago in the Mediterranean.

By that time, due to isolation from the Indian and Atlantic oceans, the Mediterranean Sea had dried up, turning into a vast and shallow basin. Its bottom was gradually filled with a three-kilometer layer of gypsum and salt, formed during the evaporation of sea water, and in the warm brines of shallow lakes, preserved in some places, only special bacteria - haloarchaea - could survive. This stage in the history of the region is called the Messinian crisis. 5.33 million years ago, the waters of the Atlantic Ocean began to penetrate through tectonic cracks through the western side of the basin.

The water cut a fairly wide channel through the rocks - the present-day Strait of Gibraltar - and poured into the dry, saline lowland. The filling of the Mediterranean Sea occurred very quickly, only 15–20 thousand years, during which ordinary marine organisms settled in it.

For a long time, global catastrophes that could influence the evolution of earthly life were of little interest to scientists. It was more important for biologists and geologists to understand the progressive and continuous change of species. Only in the middle of the 20th century, when it was established that mass extinctions coincide in time with catastrophic events, such as outbreaks of volcanism and meteorite falls, they began to be studied purposefully.

Global disasters occurred on Earth quite often. The theory of evolution is based on data from paleontology, a science that studies the preserved remains of living beings. Paleontology uses the geochronological time scale, adopted in 1881 in Bologna at the International Geological Congress, which reflects the main dates in the history of our planet.

The most ancient part of Earth's history is called the Cryptozoic. It covers the interval from 570 to 3800 million years ago. During this period, organic life was in a latent state. The next part, 570 million years long, is called the Phanerozoic. The Phanerozoic is divided into three eras: the Paleozoic (the era of “ancient life”), the Mesozoic (the era of “intermediate life”) and the Cenozoic (the era of “new life”). Eras are divided into periods. The first living organisms appeared on Earth approximately 3.5 billion years ago. These were the simplest creatures - microorganisms. The Cambrian period was characterized by organisms of higher complexity.

Life developed mainly in the seas and was represented by primitive crustaceans, mollusks, and corals. Marine vertebrates - shield fish, starfish, etc. - appeared 450 million years ago.

Life, which developed rapidly in the seas during the Ordovician period, began to fade away 440 million years ago due to the onset of glaciation. In the Silurian and Devonian, life first reached land. Significant changes in the appearance of the planet resulted from the enrichment of the Earth's vegetation cover with trees and shrubs that produce seeds, which occurred approximately 360–385 million years ago. It is believed that hundreds of thousands of years ago it was enough for vast forests to cover the previously bare rocks, sands and lands of all continents.

The most massive extinction of living beings in the entire history of our planet occurred 251 million years ago, at the end of the Paleozoic era. Over 90%

of marine and 70% of terrestrial species disappeared forever from the face of the Earth - only the smallest and most primitive remained.

In the World Ocean, the formation of reefs, which had hitherto been widespread throughout all seas, ceased, and on land, the accumulation of coal ceased, since the lush forests of tree-like mosses, ferns and various ancient gymnosperms that covered it disappeared.

Some terrestrial amphibians survived, as well as reptiles, for example, proterosuchians - the ancestors of dinosaurs, cynodonts - animal-like lizards, the ancestors of mammals, and lystrosaurs - their distant relatives. These were small animals that required less energy expenditure to maintain activity, which means they consumed less oxygen. Among marine animals, the smallest foraminifera, brachiopods, and bivalves also survived the catastrophe, since they required less food and oxygen.

The terrestrial flora suffered no less than the fauna - chlorine-containing emissions from volcanoes destroyed the ozone layer, harsh ultraviolet radiation crippled spores that had not yet germinated, sulfuric acid rains burned out foliage, and the last juices from dying trees sucked out the proliferating mushrooms. The previous level of biodiversity on Earth was restored only 60 million years later, by the middle of the Jurassic period.

The flora and fauna died due to a lack of oxygen, which arose during the decomposition of dead organic matter left by the ocean when it retreated from the mainland. Waste from the forests was carried into the sea. Huge plantations of algae were formed, which, dying, fell to the bottom. The process of their decomposition absorbed the oxygen in the water. The inhabitants of the oceans began to suffocate, the seabed was empty. As a result, the Permian period ended with a grandiose cataclysm.

Among the external causes of extinction, scientists also name a catastrophe caused by powerful volcanic eruptions in Eastern and partly Western Siberia. It was a short-term event on a geological scale that greatly affected the biosphere. Its traces are captured in the form of a vast mass of basalts, several kilometers thick, called the Siberian traps.

The last global catastrophe in the history of the Earth occurred 65.5 million years ago. The cause of the disaster was a giant meteorite that fell to Earth. The meteorite was about 10 km long and crashed into the Earth at a speed of 20 km. per second and left a pit 20 km deep. The crash site of this celestial body is the northern coast of the Yucotan Peninsula in Mexico. This is evidenced by the Chicxulub crater located there, the time of its appearance approximately coincides with this event. A monstrous explosion occurred, accompanied by a release of energy 10,000 times greater than all current nuclear reserves.

As a result of a powerful cataclysm, 100 billion tons of sulfur were released into the atmosphere, the air was filled with sulfur compounds, and forests were engulfed in giant fires. Most of the Mesozoic inhabitants who lived then died from shock and heat waves, toxic emissions, acid rain, hurricanes and tsunamis. Clouds of dust and clouds of smoke that rose into the atmosphere enveloped the planet for many months. They reflected the sun's rays; As a result, a sharp cooling began, and vegetation, left without light and heat, began to die.

Then there was a mass extinction of animals deprived of food. This disaster is associated with the death of 35% of the species that inhabit the oceans, as well as all large reptiles: sea lizards, dinosaurs and pterosaurs.

In neo-catastrophism - this is what the updated theory of Georges Cuvier is now called - there are a lot of assumptions that still do not have reliable empirical evidence. If the existence of eras of powerful volcanism, which left noticeable traces in the earth’s crust, is beyond doubt, then proving the fall of an asteroid and establishing the time of its explosion is not so simple.

In addition, it is extremely difficult to understand how the consequences of the disaster led to the extinction of species. There is also no answer to the question why some major cataclysms (for example, basaltic outpourings in

South America and Africa 130 million years ago) did not lead to the mass extinction of living organisms.

Not for all powerful catastrophes in the history of the Earth that led to the death of animals and plants (there are six of them) it was possible to find biological, geological and cosmic causes. With every global catastrophe, along with the defeated species, there were also winners, who subsequently filled the vacated living space. But not a single species was involved either in the disaster itself or in the survival of other species.

The global catastrophe threatening the Earth, if it occurs, will probably be associated not with the influence of external cosmic forces or internal processes in the earth's crust and biosphere, but with human activity.

MAN AS A SOURCE OF DANGER

Over time they became dangers appear, the creator of which became the man himself. Man lives and acts in conditions of constantly changing potential dangers. This allows us to formulate axiom that any activity or inactivity is potentially dangerous. Currently a person suffers most from his activities, from the dangers he himself created.

As the pace of technology accelerates progress impact of economic human activities on the environment the environment is becoming increasingly destructive. More and more is getting into nature and more substances alien to her, sometimes highly toxic to living organisms.

A person from a position of security vital activity must be considered as a potentially dangerous factor, whose impact on others objects can take them beyond the limits sustainability. There are two features manifestations of human impact to the natural environment: the technological development of mankind is accompanied by transferring more and more to a person number of control functions, allowing he is moving further and further away from the guns labor and turn from performing to the governing body of the system production.

Such a transformation human role leads to the replacement of physical mental labor, reducing the need muscular work and corresponding energy costs. However, this significantly increases burden on the human psyche.

The main culprit of accidents is, as a rule, not a technique, not an organization labor, but the working person himself, who for one reason or another did not follow the rules safety precautions.

More than 60% of the unhappy cases are explained by ignorance or violation labor safety requirements discipline, unsatisfactory organization production.

General consideration of patterns development and human life allows us to notice that the circumstances conducive to growth number of accidents that occur according to quite objective reasons. The first reason is revealed from an analysis of human evolution. With the development of tools, the range of human impact on the environment world.

At the same time, the range of responses expanded reactions from the outside world. If primitive a person according to his individual physical was able to withstand the possibilities arising at that time in the labor process activities dangers, then opportunities modern man is significantly behind on the level of increased danger. With development technology danger is growing faster than human opposition to it. The second reason making the conditions human labor and life are more stringent and dangerous is the increase in the cost of error.

Retribution for the mistake of primitive man was not so great, but the mistakes of modern people cost him much more. The third reason is human adaptation to danger. Using the benefits given technology, people often forget that technology is usually also a source high danger, and intensive use it increases the possibility of dangers being realized.

Often due to current small benefits a person deliberately commits a violation safety rules. Not everyone violation entails accident happening. People who once violated with impunity rules and having received due to this some benefits, repeat similar violations.

Gradually adaptation occurs not only to danger, but also to violations of the rules security. In addition to the general reasons, it is found many individual factors contributing to deliberate violations of safety rules labor and an increase in the number of accidents.

Issues related to manifestations of humanity factors are considered as an analysis of human reliability, which includes determining potential sources of human errors throughout the entire period preceding accidents. These errors can be divided to mistakes, oversights and manifestations of evil intent.

A significant proportion of dangers are realized under the influence and direct participation of the person himself, conditioned his behavior, existing psychophysiological features and capabilities human body. So, 45% of accidents at nuclear power plants, 60% of plane crashes, 80% of maritime accidents and 90% of car accidents occur solely through the fault of the service provider personnel for various reasons.

Causes of hazardous situations and work-related injuries, related to the human factor, can be broken down into different levels: under the same circumstances for all workers, determining value in shaping the behavior of each person have its individual qualities, reflecting a set of socio-psychological and physiological properties. These include type of nervous system, temperament, character, features of thinking, education, experience, education, health and other qualities.

A wide range of personality traits, social circumstances and production conditions labor is formed by psychological reasons deliberate violation of safety rules work. In every action a person is distinguished three functional parts: motivational, indicative and executive.

Violation in any of these parts entails a violation of the action generally. Man breaks the rules and instructions. He does not want to follow them, either he doesn't know how to do it, or he is unable to do this.

Since the 90s of the twentieth century, it has become increasingly widespread new concept - safety culture, which provides the main role human factor in the security system.

This required her to think about it comprehensive analysis and development of fundamentally new approaches, criteria and methods for ensuring security. An error is the result of an action performed inaccurately or incorrectly, contrary to the plan.

In cases where dangerous or inappropriate actions are committed by a person consciously (intentionally), they are classified as violations and are not analyzed in this text.

An error is defined as the failure to complete a task (or a person performing a prohibited action) that can cause serious consequences - injury, death, damage to equipment or property, or disruption of the normal course of planned operations.

Errors due to a person’s fault can occur in various areas and conditions of his life: on vacation, while traveling, while playing sports. For example, errors often occur when driving vehicles; careless handling of fire, sharp objects, or weapons; when swimming in bodies of water; when traveling in the mountains; during training and competitions in various sports.

In everyday life, mistakes occur when using electrical appliances, household gas, and open fire. They occur when using pesticides, tools and devices; when handling household waste, boiling liquids, and items containing mercury; when consuming low-quality products, alcohol, medicines, etc.

In the field of production activities, errors occur if a person acts in violation of the established work schedule or is inactive at the moment when his participation in the activity process is necessary.

In emergency situations of natural and man-made origin, errors are usually associated with people’s unpreparedness to act in emergency situations; with their inability to foresee the results of their actions, for example, when handling flammable and explosive substances or when managing complex technical systems; during avalanches, mudflows, etc.

When people communicate with each other, sources of errors can be dishonesty, negligence, revenge, jealousy, insults, religious and national conflicts, etc. When managing the economy and other government activities, mistakes are often caused by people’s desire to violate the laws of nature. These include the construction of a pulp and paper mill on the island of Baikal; projects for turning the Northern rivers to the south, etc.

A person’s ability to make mistakes is a function of his psychological state, and the intensity of errors largely depends on the state of the external environment and the current loads. It has been established that the dependence of the error rate on the current loads is nonlinear. Thus, at a very low level of load, most operators work ineffectively (the task seems boring and does not arouse interest), and the quality of work is far from desired.

At moderate loads, the quality of the operator's work is optimal, so moderate load can be considered as conditions sufficient to ensure attentive work of the human operator. With a further increase in loads, the quality of a person’s work deteriorates again, which is explained mainly by manifestations of physical stress, such as fear, anxiety, increased heart rate and breathing rate, increased temperature, release of adrenaline into the blood, etc.

In the “man - environment” system, man is the most variable component. His behavior is determined by a number of individual factors. Often different operators perform similar tasks using different actions.

The main features of the personality and state of the human body that push him to make mistakes can be divided into congenital features and temporary conditions.

Congenital characteristics include the physiological characteristics of a person and characteristics due to his heredity. These include the senses (hearing, vision, smell, touch, taste), the musculoskeletal system (muscle strength, speed of movement, coordination, etc.). This can also include the human psychomotor system (reflexes, reactions, etc.) and his intelligence (level of knowledge, ability to navigate the environment).

Temporary conditions, such as physical and psychological fatigue, leading to decreased attention and muscle strength, deterioration of health and performance, contribute to the occurrence of errors. Factors that distract attention include temporary functional disorders of the body (for example, an unexpected acute headache, dizziness, muscle cramp, etc.); temporary switching of attention to some event or object not related to work; fatigue; sudden external influence (noise or bright flash of light).

THE CAUSES OF ERRORS ARE DIVIDED INTO IMMEDIATE, MAIN AND CONTRIBUTING

Direct errors depend on the psychological structure of the operator's actions. These are errors of perception errors of memory and errors of thinking (did not understand, did not foresee and did not generalize).

The main causes of errors are related to the workplace, labor organization, operator training, the state of the body, the psychological attitude, and the mental state of the body. Contributing causes of errors depend on personality characteristics (character, temperament and communication characteristics), health status, external conditions, professional selection, education and training.

The causes of errors can also be classified using a cybernetic scheme: errors in orientation (failure to receive information); errors in decision making (wrong decisions); errors in performing actions (incorrect actions).

Errors in orientation are the most common and usually arise due to the absence of a signal, due to a weak signal, or due to many simultaneous signals.

Errors in decision-making can occur when all the necessary, reliable information has been received in sufficient volume, but the process of analyzing, processing and comprehending it was incorrect; or due to an inadequate assessment of the situation; inability to work due to lack of knowledge and experience.

And sometimes the information and the decision made may be correct, but the response is wrong. An incorrect action can also manifest itself in the operator's inaction at the moment when his action is necessary (inability to act, violation of the sequence of actions), or in the wrong choice of actions (inadequate arrangement of instruments, lack of attention, fatigue, etc.).

The types of errors made by humans at various stages of creating and using technical systems can be classified as follows. Design errors are caused by unsatisfactory design quality. For example, controls and indicators may be located so far apart that the operator has difficulty using them at the same time.

Manufacturing and repair errors may occur, for example, incorrect welding, incorrect choice of material, manufacturing of a product with deviations from design documentation; maintenance errors during operation due to insufficient training of maintenance personnel, unsatisfactory equipment with the necessary equipment and tools.

Handling errors may also occur. They arise as a result of unsatisfactory storage of products or their transportation with deviations from the manufacturer's recommendations. Errors in the organization of the workplace include cramped working space, increased temperature, noise and insufficient lighting. Errors in team management lead to insufficient stimulation of specialists and their psychological incompatibility.

Damage to the body occurs, which, when a certain degree of change is achieved, is classified as an accident (injury) or disease. Damage to the body can occur as a result of both direct contact external influences (mechanical, electrical and chemical) and remote (thermal and light).

Damage may occur immediately after exposure or some time after exposure (for example, after radiation exposure). Dangerous and harmful factors usually have externally defined spatial areas of their manifestation, the so-called dangerous zones. Finding a person in a dangerous zone is one of the conditions for damage to the body. In this case, the dangerous factor (danger) must have sufficient energy to cause damage to the body.

But in most cases, people themselves do not attach due importance to the hidden danger and act to their own detriment. A typical example of a disregard for danger is violating traffic rules. Hazards can manifest themselves in the form of breakdowns of technical systems, fires, explosions and other events that are difficult to predict. When exposed to such extreme situations, people risk receiving injuries of varying severity.

Man himself is often a source of danger. By his actions or inaction, he can create a real threat to life and health for himself and others. The dangers created by humans are very diverse. Wars, conflicts, crimes, prostitution, drug addiction, hunger, poverty and lack of culture in human society form social dangers.

No matter what activity a person engages in, no matter where he is, there are always hidden forces next to him that pose a threat to him. The cause of an accident is often the carelessness or carelessness of others. To preserve health and life, it is necessary to know well and promptly eliminate the reasons why potential dangers turn into actual dangers.

It is not always possible to protect yourself from misfortune, since some dangers do not depend on people’s actions and appear suddenly, leaving no time for reflection or rescue, for example, explosion, earthquake and hurricane.

Hazard can be assessed quantitatively, for example, by the magnitude of the risk. Risk as a quantitative measure of danger usually means the possibility (or probability) of an undesirable event occurring over a certain period of time. Risks include car accidents, crime, poisoning, intentional homicide, drowning, falls, fire and burns, and plane crashes.

CRIMINAL DANGERS AND VICTIMOLOGY

Victimology is the study of victim behavior, which explains what motivates a street robber or rapist when choosing a victim.

Betty Grayson, through a series of studies, has shown that it takes an average of seven seconds for a criminal to visually assess a potential target for attack - his physical fitness and temperament. The offender notes uncertainty in his gaze, sluggish posture, timid movements, mental depression, physical disabilities and fatigue. As a result of mathematical analysis, it turned out that criminals often identify potential victims based on certain distinctive features and movements. It may be their general inconsistency, the clumsiness of their gait - too sweeping or mincing, which attracts attention against the backdrop of a single stream of people.

Joel Kirch and George Leonardo identified two general categories of people: the so-called “at-risk group” and those who are in virtually no danger of becoming the target of an attack. The first of them are poorly physically organized, relaxed and mentally uncollected. The second ones are confident in themselves. They look and walk with confidence. A person who feels he belongs to a risk group should first study his own gait, gestures and facial expressions and begin to correct them. Anyone can instill a confident style of behavior in themselves and follow it among the street crowd.

DIGITAL VIOLENCE

Digital violence refers to manipulative actions against a person for the purpose of control, intimidation or harm using Internet platforms. Such violence is common today in the family, at school, university, at work, and on dating apps. Digital violence can come in many forms. If this concerns children unde 18 years of age then cyberbullying and cybergrooming are more common.

Women face upskirting (taking photos of private parts without consent), slut shaming (when others judge a woman's attempts to look attractive and sexy) and revenge porn (posting sexually explicit material online without the consent of the people depicted in it). Statistically, women experience digital violence more often than men.

Digital violence in partnerships is particularly difficult to recognize. It is often disguised as concern: “Why don’t you pick up the phone? I’m worried” or “Where are you? Half an hour has already passed and you are still not at home.” In these cases, the partner tries to subjugate the other partner, control him and become the main one in the couple. Therefore, it is easier for the second partner to constantly inform where he is and with whom respond in a timely manner in instant messengers, and show correspondence with friends.

How digital violence manifests itself. Without asking permission, your partner uses your phone: reads correspondence, checks the log of calls and messages. Your partner is watching you: without your knowledge, he installs location tracking apps on your phone or hidden cameras in your apartment. The partner controls your access to Internet platforms, asks for passwords and codes, decide with whom you should communicate and with whom you should not. Your partner is constantly trying to stay in touch with you.

Calls and messages every 5-10 minutes demanding to send photos of the people who are near you and the places where you are Your partner shares intimate photos or videos with you, even if you didn’t ask for it, and expects the same in return. Your partner threatens to share your intimate photos with the public in order to renew the relationship or to extort money. Your partner posted explicit photos of you online to insult or humiliate you.

How to avoid digital violence

1. Agree with your partner about the boundaries of what is permitted

Respecting personal boundaries is an indicator of a healthy relationship. For some, one SMS or call is enough for the whole day, while others need to correspond much more often. This needs to be discussed with your partner.

2. Remember that you decide what you do.

Even if your partner insists and you don’t want to, you have the right not to do it. This applies to any action. You defend your personal boundaries; there is no shame or inconvenience for this. You should be safe.

3. Don't forget that it's almost impossible to remove something from the Internet.

This is especially true for candid photos and videos. When sharing such media with someone, make sure it is safe for you to do so. Otherwise, this may become a reason for blackmail or revenge on the former partner.

4. Maintain confidentiality

Passwords must be strong. Some apps now work with two-factor authentication. Smartphones can be unlocked not only using a digital code, but also using a fingerprint or facial recognition function. If there are applications on your phone for tracking geolocation, then it is better to delete them.

What to do if you experience digital violence

• Talk to your partner again about personal boundaries.

• Be careful with the information you provide to your partner (photos, videos, audio files).

• Record conversations with your partner take screenshots during correspondence if you receive insults, humiliation or threats.

• Share your experiences with someone: relatives, friends, psychologists, support centers.

• Create a new account on social networks, change your email.

• Uncheck "Show my location" in your phone settings.

• Ask your friends not to post media files with your presence.

Digital violence has a huge impact on mental health. People stop trusting, are afraid of new relationships, and withdraw into themselves. Digital violence can be encountered on dating apps. Actors of such violence can be strangers or acquaintances and even close people: relatives or partners.

Even if you trust your partner or know that he will immediately delete the material, it is still unsafe to send intimate photos because data about them may remain on the Internet.

For gadgets and social networks, choose a strong password, two-factor identification, unlocking devices and applications using a fingerprint or Face ID.

Check to see if your devices have spyware that tracks geolocation. Signs of the presence of stalkerware may include a sharp deterioration in performance, changes in settings without your knowledge, the appearance of unfamiliar applications, and crashes in programs that previously worked normally.

Try to clarify the situation through dialogue first, if possible and safe. It happens that there is a misunderstanding. For example, a person believes that calling his partner every hour and asking about his affairs is correct. He may not realize that for the second person in the couple this looks like attempts at control or pressure. If it becomes clear that the partner considers what is happening to be the norm and thus seeks to establish his control in the relationship:

Be careful with the information you want to share, be it a text, a voice message, a photo. Seek help from relatives, friends, and domestic violence specialists. It's important to share what's going on, even if you can't leave. Contact a psychologist to help you create a safety plan. You can consult with a lawyer: if the actions of the violent actor fall under some article of the Criminal Code, he will help you prepare documents for the court.

Make recordings of telephone conversations, screenshots of correspondence in which you are insulted, blackmailed, or threatened. If possible, create new email, social network, and instant messenger accounts from a device that only you can access. Use the browser in incognito mode, which will not save your search history.

Check your phone settings. It is better to turn off location display altogether or leave it only when using a specific application. It is worth changing passwords and PIN codes periodically, even if they are different for different applications and accounts. Set up two-factor authentication where possible, and check your phone's privacy settings to see which apps you allow to store information about the location and time of the photo.

Ask your loved ones not to share information about you on social networks. Don't let them post photos of you or tag places they've been to with you.

If the relationship is over, the violence has stopped.

Monitor your mental health. Some consequences appear immediately, while others, such as symptoms of PTSD, may occur within six months. If you observe changes in your psycho-emotional state, try to seek help from a psychologist. If you suspect surveillance, you may need a digital security specialist. You should be wary if your partner or ex-partner shows up in a place and at a time that he had no way of knowing about. Or he seems to accidentally pronounce words from your dialogue with other people, casually asking about the place that you discussed with your interlocutor. Sometimes violent actors can simply send screenshots of your location or conversations with other people, manipulating that they know everything about you. You can check your car at a repair shop for tracking devices, and take the gadgets to a computer technician.

Identify your feelings and thoughts about what happened. Remember that all your reactions are normal reactions to abnormal circumstances.

Remind yourself of your strengths and accomplishments that remain the same despite the abuse you have experienced.

Practice self-care: try to get enough sleep, eat well include activities that you enjoy in your daily routine: yoga, running, meditation, listening to music drawing. Avoid self-blame. It's better to invest your energy in the things you can control in your life. Perhaps rethinking the experience and learning the skills of setting personal boundaries will help.

Practice self-compassion: be kind to yourself, be aware of your thoughts and feelings, and learn to accept your imperfections without judgment. Avoid substance abuse and anything that can cause you physical or emotional harm.

Don't hesitate to seek professional help.

Look for support where you will be heard, understood and accepted. Digital violence can leave the same traumatic mark as more obvious violence in the form of insults, threats, and beatings, Parsadanian explains. But in some cases, according to the expert, it can have an even stronger impact, because digital violence can be committed anonymously, at any time and in any place. Because of this, the injured party may not understand the connection between the offender's actions and changes in their psychological state.

Digital violence can continue even if the violent actor no longer takes any action. The Internet remembers everything, so if a person only once posted intimate photographs of the victim online and did nothing else, these images can continue to spread online for a very long time.

Consequences of digital violence: High level of anxiety; Depression; Panic attacks; Problems concentrating; Decreased self-esteem and quality of life in general; Forming a negative outlook on the future; Lack of trust; Attempts to isolate yourself from communication with other people; Feeling unable to take control of life back; Substance abuse; The appearance of symptoms of post-traumatic stress disorder (PTSD).

Legal protection from digital violence is difficult. There are more and more digital tools and methods for control, influence and intimidation in the online environment, but legislation is changing slowly.

Thus, in 2009, the Philippines became one of the first countries to introduce criminal liability for such actions: a person can go to prison for three years for publishing someone else's intimate materials. In England and Wales, revenge porn became a crime in April 2015, punishable by up to two years in prison. And in Israel in 2014, the publication of intimate photographs without the consent of those depicted in them was recognized as a sexualized crime. It is punishable by up to 5 years in prison. 40% of Internet users have suffered from digital abuse at least once, and 73% have witnessed it.

While men are more likely to experience online abuse, women are more susceptible to sexualized harassment and online stalking. The most vulnerable group is young women aged 18 to 24 they account for about 70% of online harassment cases. 54% of women who reported being digitally abused knew their abuser. Digital violence can accompany partnerships and co-exist alongside other types of violence.

Women, in an attempt to protect themselves from online harassment, cyberbullying and other manifestations of digital violence, are depriving themselves of full access to information, work, education, health care and communication. 60% of people who experience digital violence ignore it, but 40% try to counter it, mostly by responding to or blocking the offender. However, only one in four women reported the misconduct to the administration of the online platform on which it occurred. Mostly, victims seek support from family and friends, because often they cannot be held accountable for manifestations of online abuse.

To contact the police, lawyers advise documenting the violence experienced as much as possible: taking screenshots, screen recordings, saving images, threatening audio and other materials that will help prove the guilt of the violent actor. Forbes Woman talks about concepts that describe ways of carrying out digital violence.

DICTIONARY OF DIGITAL VIOLENCE

Upskirting: filming the intimate parts of the body of an unknown woman or partner without consent. Upskirting does not take place in virtual space, but using a phone or any other camera. There is a known case when a man, in order to remain unnoticed, attached a miniature camera to his shoe. One of the latest high-profile cases of upskirting is the arrest of a former employee of the Disney World amusement park, who during six years of work at the park took more than 500 photographs and videos of women “upskirt.” In Russia, upskirting is not recognized as an offense and does not entail liability, although many countries are gradually introducing penalties for filming up to a real term.

Doxing: Publishing sensitive personal information online - home address, email address, phone number, documents - for the purpose of harassment, intimidation or extortion. In 2014, American video game developer Zoe Quinn became a victim of doxxing. The guy she broke up with posted a blog post accusing Quinn of cheating on him with a journalist to get positive press for her work. This began a whole campaign of online doxxing of developers: they received threats of violence, rape and even murder - this scandal was called “Gamergate”. “The hackers weren’t just sending me death calls or telling me what a fat slut I was, they were sharing my personal information: my old address in Canada, my old cell phone numbers, my current cell phone number and my current home address,” Quinn said about the experience.

Zoom-bombing: hijacking a video conference and interrupting communication by playing video (often pornography), audio, or broadcasting one's own screen. Digital violence has worsened amid the coronavirus pandemic in 2020, as people spent more time online socializing and working. At the same time, the first cases of Zoombombing were recorded as the Zoom platform gained popularity. Cyberstalking: continuous offensive behavior towards an Internet user, intrusive sending of messages, photos and videos, including threats, in order to intimidate him. Online stalking can continue for years.

It happens that a cyberstalker stalks a victim in real life: for example, by installing a GPS tracker or simply tracking a person using social networks, geotags and photographs. Around 26% of young women aged 18–24 have experienced online stalking.

Cyberbullying: bullying using digital technologies. This includes, for example, offensive messages, be it personal correspondence, a comment under a photo, or interaction on a forum.

Cyberbullying can also manifest itself through threats - when a person states their intention to cause bodily harm or even kill another. Women are often intimidated by threats of sexualized violence, including rape.

Online trafficking: human trafficking using the Internet, mainly social networks. The Internet has become a convenient tool for traffickers around the world, 72% of whose victims are women and girls. At the same time, 77% of women identified among victims of trafficking were sold into sexual slavery. Due to the coronavirus pandemic and border closures, human traffickers have become more active online and are increasingly seeking victims for sexual exploitation on the Internet, including through webcams and online pornography.

One of the preferred methods for finding victims of online trafficking has become the posting of fake job offers that promise job opportunities, often in distant countries. Targeting facilitates the spread of such recruitment. The anonymity and speed of information transfer online allows criminals to quietly and quickly arrange the transportation and accommodation of victims, as well as hide the proceeds of their crimes.

Revenge porn: publishing intimate videos or photographs for the purpose of revenge, usually against an ex-partner or spouse. Revenge porn can be based on deepfake: using artificial intelligence, an image, audio or video can be created that believably imitates a person's appearance or voice.

Swatting: This is a false call to a victim's house by a SWAT team, a squad of police in full force, under the pretext that she is in serious danger. A cyberstalker may resort to swatting. The word comes from SWAT, the name of a division of American law enforcement agencies.

Sexting: Sharing intimate messages and photos is not only enjoyable roleplay, but also a big risk. Sexting can become sexualized violence when a partner asks for photos against the woman's will. A person who receives nude photos can publish them, use them for blackmail or for revenge after a breakup or quarrel. Sextortion: blackmail through intimate photographs and videos that the author of the violence threatens to post on social networks and send to colleagues, relatives or friends of the victim if she does not agree to his terms.

The author of violence may also send the victim unsolicited nude photos and videos, write messages to her with sexualized overtones or direct messages of a sexual nature. The most common types of digital violence are: online stalking - sending unwanted emails, audio/video or text messages, intrusive calls, location tracking;

Online harassment is a broader category of threats or other offensive behavior aimed at humiliating, belittling, or insulting individuals in online public spaces and private messages; cyberbullying - combines aspects of online stalking and online harassment, most often found among teenagers and committed by a group of individuals; creepshot (English creepshot, that is, “ugly shot”) and upskirting (English upskirting, literally translated as “under the skirt”) - creating photos/videos of the intimate parts of the body of a partner or unfamiliar women (back, buttocks, legs, neckline) without their consent; cybergrooming - the affection of a child/teenager by an adult in order to establish trust for further sexual relations; hacking a computer or other technical devices without the consent of the owner - usually hacking a webcam, which most often negatively affects women; sexualized violence based on photo/video images - creation, transmission, distribution of these materials without the consent of the victim.

It is important to consider that she could have consented to the shooting of photo/video content. Often leads to self-blame if images were shared without consent. Includes revenge porn (including with the disclosure of personal data), sextortion (abuse of power to obtain “sexual gain” or some advantages associated with it), deepfakes (faking images using artificial intelligence technologies); libel - intentionally causing damage to a person and/or reputation through making false statements (for example, spreading rumors on social networks); slut shaming is online criticism of people, usually women and girls, who violate expectations of behavior and appearance associated with their sexuality; online trafficking - trafficking in people, especially women, using technology and social networks, often leading to prostitution.

The highest level of damage is caused to mental health. A woman may experience anxiety, depression, panic attacks problems concentrating, decreased self-esteem and decreased quality of life in general.

In cases of digital sexualized violence, for example, the production and distribution of intimate photos/videos without the victim's permission, the consequences can be even more serious: depression, which can lead to substance abuse, PTSD symptoms. The victim may isolate herself from communication with other people, including online, experience feelings of guilt and shame, feel lonely and think that no one will believe her. There is also the potential for digital violence to escalate into offline violence, for example in cases of online stalking or threats of harm to life or health.

Factors that help to recover faster after violent exposure are the opportunity to share the experience with loved ones and safe people, attend thematic support groups, and receive psychological and, if necessary, legal assistance from a specialist. If knowingly false information is disseminated about you, discrediting your honor and dignity or undermining your reputation, there is criminal liability for this. Knowingly false information is considered to be information that does not correspond to reality, claims facts (that is, it must not be a value judgment or opinion of a person) or events that did not take place in reality, for example, the commission of a crime or the presence of a disease.

Knowledge is a mandatory sign, which assumes that the person knew for sure that the information he was reporting was false.

If the aggressor distributes (for example, transmits screenshots, including in printed form, sends them by email, on social networks or instant messengers, publishes on various websites) your intimate photographs, videos or other information that constitutes your personal or family secret, his actions fall under this article. This may also include the illegal collection of information about your private life, which constitutes your personal or family secret, without your consent. Illegal collection may mean, for example, the theft or illegal acquisition of information: handle the information you want to share carefully: text, voice message and photo; seek help from family, friends and domestic violence specialists. It's important to share what's happening, even if you can't leave.

Contacting a psychologist will help you draw up a safety plan, consulting a lawyer will help you prepare documents to submit to court if the offender's actions constitute an offense or crime; make recordings of telephone conversations, screenshots of correspondence that contain or may contain threats, insults, blackmail; create new email, social network, and instant messenger accounts from a device that only you have access to; use the browser in incognito mode so as not to store your search history;

Check your phone settings: location and privacy. It is better to turn off location settings altogether or leave them only when using specific applications. In your privacy settings, specify which applications you have allowed to store information about the location and time of shooting; change your passwords and PIN codes, make them different for different applications and accounts. Set up two-factor authentication where possible; check who can tag you in photos and videos; ask your loved ones not to share information about you online for your safety. If necessary, you can ask colleagues and classmates about this.

About 55% of dating app users haved experienced various types of security breaches. Fraudsters on dating apps can be identified by their behavior patterns. They often provoke frank conversations and try to transfer communication to other platforms too quickly. Application developers are trying to build protection for their users. If the algorithm sees that a conversation could potentially become dangerous, it sends a warning alert with recommendations on how to protect yourself.

Dating apps are becoming like social networks. Here you can not only meet for relationships, but also find like-minded people, roommates and friends. If previously the goal of dating service developers was only to create a couple and get people to communicate on social networks, now they create their own messengers and support users at the entire stage of the relationship. Application creators are striving for gamification of services. In the future, communication in augmented reality rooms will become a popular way of communication. People will be able to change avatars and rooms according to their mood.

THE CONCEPT OF A SOURCE OF INCREASED DANGER

Power determines the ability of a source of increased danger to cause significant damage, and complexity determines its relative reliability. A feature of the source of increased danger is the uncertainty of the development of the process. A high probability of causing harm to others is identified as a sign of a source of increased danger.

It seems to us that the most important feature of some sources of increased danger is the irreversibility of the destructive process that they cause. Once the source begins to function, it is no longer possible or very difficult to intervene in the course of events and change the development of this process. Let's take a nuclear reaction as an example.

Depending on the origin, the source of danger can be: natural, anthropogenic or mixed - natural and anthropogenic. Natural ones include: earthquakes, eruptions, hurricanes, floods, lightning, wild animals (animals, snakes), poisonous plants and mineral poisons. A significant and rapidly growing share of hazard sources is of anthropogenic origin, that is, it is a product of humans and their activities. No wonder the ancients argued that man is his own worst enemy.

In civil law, there are two approaches to determining the source of increased danger, which are designated by the terms “object theory” and “activity theory.” In accordance with the first of them, sources of increased danger are considered to be objects of the material world that have properties that are dangerous to others and that cannot be fully controlled by humans.

A source of increased danger should be recognized as any activity, the implementation of which gives an increased likelihood of causing harm due to the impossibility of full human control over it, as well as activities involving the use, transportation, storage of objects, substances and other objects of production, economic or other purposes, having the same properties.

A source of increased danger is a property of one, most often unstable, system (substance, mechanism, phenomenon, process, organism, personality, social group), the development or manifestation of which is weak or uncontrollable and can produce irreversible destructive changes in this or another system.

This source has a high damaging effect, great concentrated internal energy, and enormous destructive power. The destructive process that has begun is poorly controlled or completely uncontrollable, and its consequences are often irreversible.

The traditional “civilistic” interpretation and the “list” approach, according to which sources of increased danger include various objects (substances, types of flora and fauna, products of human activity) or certain types of activities, are narrow and do not cover the entire variety of sources of increased danger. There is a need to develop a definition of the source of increased danger, which would have general legal and criminological significance.

In principle, any human activity is both useful and harmful. The axiom of the potential danger of human activity is formulated, from which two most important conclusions follow:

1) it is impossible to develop an absolutely safe type of human activity,

2) there can be zero risks in any type of human activity.

However, some types of activities objectively pose a greater danger than others. For example, criminal activity. They distinguish “source of criminal danger”, “criminal danger”, meaning the danger from crime. The activities of terrorist organizations have obvious signs of a source of increased danger.

Products of human activity can also be a source of danger. This group includes most narcotic drugs, psychotropic substances, radioactive materials, weapons, hazardous production facilities and dangerous goods.

Sources have appeared, the danger of which is not yet perceived by the public consciousness. For example, one of the most powerful unstudied and therefore unpredictable sources of danger is electromagnetic pollution. With the development of computer technology, their social significance is growing, but, unfortunately, so is their potential danger. In the modern information society, computer virus epidemics can be sources of increased danger.

Social sources of psychological danger deserve special attention. The source of increased danger may be an individual, a social group or another subject of activity and management. After all, any activity presupposes not only an object, but also a subject.

From the standpoint of the theory of the subject, certain personal properties of biological origin or formed under the influence of negative social factors can act as special sources of danger. These include social danger, which was formed as a result of mental illness or caused by negative moral and social qualities, cruelty, self-interest and other individualistic attitudes.

The source of increased danger can be a criminogenic personality, which is expressed in the totality of the properties and qualities of the subject, indicating a predisposition to commit a crime and repeat it. The mental properties of a person can act as a source of danger during the transformation of mental energy into the energy of a socially dangerous act, through mental intervention, for example, of a hypnotic, psychic nature.

Sources of increased danger are criminal, terrorist, and extremist organizations. Subjects of managerial, administrative and power relations can also be a source of increased danger. In the actual assessment and ranking of hazard sources, subjective perception plays a significant role. Very often our ideas about this are significantly distorted. Significantly more people die in car accidents than in plane crashes or at the hands of homicidal maniacs. However, Russian ordinary people tremble with horror before maniacs, but for them, driving with a drunk driver, as practice shows, is a common thing.

The second concept, which requires the same close attention of legal scholars, is an object of increased protection. This is not to say that it is not used at all in legal science. There are legislative acts on specially protected areas, protection of computer programs, cultural monuments, etc. However, the phrase “object of increased security” does not yet have the status of a general legal and criminological category.

Any system can be considered as an object of protection: an individual, a social group, society, humanity; types and products of human activity; natural objects: fauna and flora, minerals and territories, etc. The object of protection is both the material substances themselves (organisms, objects, areas of territory), and the social relations that have developed in this regard or certain activities.

The significance and value of protected objects are not the same. In the course of evolution, “nuclear” relations and main values are formed, destroying and destroying which, humanity will doom itself to death. These are the environment, knowledge, morality, law and other values. These include people of the older generation as guardians and conductors of the experience accumulated by mankind, as well as children as the future of human civilization.

The objects of increased protection should be the most important properties (relations) of the system, having lost which, it will either collapse or be transformed into another and will not be able to achieve its goal. For a system to function as a development system, its essential elements must be protected.

In the course of life, it crystallized that for the safe functioning of the individual, society and humanity, such objects of increased protection are life, health, freedom, honor, dignity, sexual integrity, property and other constitutional rights and freedoms of the individual; public health, public safety and morality; ecology, constitutional order and state security; peace and security of mankind. Essentially, these are those objects that, due to their special value, are subject to criminal legal protection.

Current legislation classifies as such specially protected territories and objects, species of flora and fauna, minerals, paleontological objects, official, commercial, state secrets and closed administrative-territorial entities.

One of the objects of increased protection should be culture, because a society can be truly safe if the absolute majority of its members are cultured and consciously and purposefully observe generally accepted norms of life.

The concept of psychological safety should consider the human psyche in two aspects: as an object of protection and as a source of danger. It follows, for example, that minors and minors, due to their intellectual, emotional and psychological immaturity, pose a threat and therefore their opportunities to enter into certain relationships should be limited, but, on the other hand, it is for this same reason that they need special protection. Restricting the legal capacity of a mentally ill person is both a means of suppressing the danger posed by him and a means of protecting his interests.

CONCEPT OF SECURITY MEASURES

To ensure the functioning of society, coercive measures have long and very widely been used, which, by their essential characteristics, do not relate to measures of legal liability (punishment) - security measures. The use of the categories “source of increased danger” and “object of increased protection” explains the social conditionality, necessity and outlines the limits of the use of this restrictive and coercive measure.

Already at the dawn of human development, it became clear that the threat of harm to the human body, the systemic principles of the organization of the community of which he is a member, must be stopped firmly and unambiguously. It is necessary to distinguish between security measures in a broad and narrow sense: security measures and security measures.

In a broad sense, security measures are the entire complex of ensuring the life of the system. For the normal existence of the human body, healthy teeth are needed, but the loss of one or even several of them will not lead to death, while the loss of the liver, heart or other vital organs will lead to immediate death.

Each system has primary elements that determine its essence and originality, and there are secondary, peripheral ones. The source poses an increased danger to the system precisely because it threatens system-forming elements. Specialized measures to protect these essential elements of the system are what we call security measures.

Law as a social regulator ensures the security of social connections through all its institutions. However, the methods of provision are different, and within the framework of the means provided by law, there are legal institutions that perform a special role - protecting the system from destruction caused by a source of increased danger. In the context of the problem under study, the entire life support complex can be called safety measures (safety measures in the broad sense), and a special legal institution for preventing the harmful influence of sources of increased danger - simply safety measures (safety measures in the narrow sense). The latter are specially created and aimed at protecting the system-forming relations of an object from the harmful effects of a source of increased danger.

Security measures are measures of non-punitive restrictions on the behavior of individuals, organizations, including legal entities, used specifically to prevent the harmful effects of a certain source of increased danger or to protect a high-security facility from the harmful influence of any sources of danger. The content of security measures consists of special duties and prohibitions that are assigned to individuals or social groups.

They arose as safety reflexes. With the development of non-genetic forms of memory, security measures were consolidated in the form of taboos, and then in the form of rules provided for in the first type of social norm, the so-called mono norm. During the development of civilization, defensive reactions crystallized into behavioral stereotypes and safety rules, the obligatory nature of which was reinforced by sanctions.

Safety rules are a set of obligations and prohibitions that a subject must observe in order to eliminate or minimize harm caused by a source of increased danger or to prevent damage to a high-security facility from any source of danger. Not all rules regulating life activities can be called safety rules. These include only the rules for a person's handling of a source of increased danger and an object of increased security.

Since power is both a source of increased danger and an object of increased security, it is quite legitimate to demand that civil servants comply with anti-corruption security rules.

As social labor was divided, two main types of sanctions emerged: incentives (positive) and restrictions (negative). The latter, in turn, are divided into sanctions of restoration (compensation), punishment and security.

Restoration sanctions are a reaction to a violation of a rule (including a safety rule), which results in damage. They are aimed at "eliminating the harm caused by an unlawful act to social relations and fulfilling unfulfilled duties." These include: enforcement of duty, reversal of illegal acts and duty to compensate for damages. Thus, the system of legal relations is recreated, violated by the non-compliance with the requirements of the law by the subjects.

This group of measures is inherent in the civil law industry. But they are also used in criminal law, where restoration is carried out through indirect incentives or by directly imposing the obligation to make amends for the harm caused. The idea of reparation, restoration of broken relationships, reconciliation between victim and offender lies at the heart of so-called restorative justice.

Punishment sanctions are the forced deprivation of certain benefits commensurate with the gravity of the offense committed. By threatening or actually causing hardship and suffering to the offender, the goals of general and special prevention are achieved. The calculation is simple: the person punished, fearing a repetition of punishment, will avoid repeating crimes, and to restrain the criminal aspirations of the majority of those around him, the experience of other people's suffering is enough.

Punishment is considered as one of the most important means of crime prevention. The mechanism of punitive action has been well studied in the legal literature. Historically, the general theory of law and branch legal sciences have a punitive emphasis and are essentially theories of responsibility-punishment, while the socio-psychological mechanism and the effectiveness of other types of legal regulation have not been sufficiently studied.

A security sanction is a reaction to the social danger of an individual, which is manifested in a socially dangerous act, or to the public danger of a social group, which is expressed in a socially dangerous activity. It is part of a social norm, which, as a consequence of socially dangerous behavior (activity) that violates a safety rule, provides for the limitation of opportunities to continue such behavior (activity). Examples of sanctions in criminal law are compulsory measures of a medical nature, some compulsory measures of educational influence, special duties imposed on a conditionally convicted person or parolee

Restriction can be carried out in different ways: physical, mechanical, organizational, psychological. Most often, security measures are implemented by imposing special prohibitions and obligations on the person who committed the unlawful act. In contrast to the safety rule, which is required to be observed by "third parties" who are in contact with the source of danger or the object of protection, a safety sanction is applied in the case when the source of danger becomes an individual, organization, social group, the danger of which has already been revealed in socially dangerous behavior or activities.

Due to the peculiarities of legislative technology, as well as due to the specialization of branches of law, security rules and sanctions can be placed not only in different articles, chapters, sections of one legal act, but also in different branches of legislation.

Security measures can be aimed at the source of danger itself (nuclear power plant), isolating or limiting its harmful effects on humans and the environment - preventive measures, or at protecting the object of protection (personality, secret, property) from external sources of danger - security measures. Since the same object can be both an object of protection and a source of danger, there may be dual-use measures that combine both the function of suppression and the function of protection - measures of suppression and protection.

The classification grounds can be the nature of the source of danger or the object of protection. If the source of danger is crime, a crime or the identity of a criminal, there is reason to highlight anti-criminal security measures.

By level, security measures can be divided into general, special and single level measures. Depending on the scope of application, security measures are classified into economic, socio-political, and ideological. Economic measures include, for example, antitrust restrictions; to socio-political – separation of powers; ideological - a ban on the propaganda of fascism.

Based on the method, physical, technical, organizational and information security measures can be distinguished. Depending on the moment of application, preventive measures can be divided into urgent and preventive. The former are used to suppress harmful effects that have already begun, the latter to suppress harmful effects that have not yet begun, but the likelihood of which is very high. Depending on the type of social norm in which the security measure is embodied, they can be divided into legal and extra-legal. Security measures in law are an intersectoral institution, adjacent to the institutions of punishment, reward, and compensation. He is represented in all areas of legislation.

According to the branch of legislation within which security measures are regulated, they can be divided into international, constitutional, administrative, civil, criminal, labor (industrial), as well as civil, administrative, criminal procedural and criminal law. executive. In international law, they make it possible to condemn the state that is the source of aggression. In constitutional law, through the separation of powers, to protect power from usurpation. In administrative law, establish special regimes regarding sources of danger (weapons) and objects of protection. In civil law, limit legal capacity. In family law, by depriving parental rights, protect a minor from harmful influences. In labor law, prevent unqualified people from entering certain professions and ensure safety precautions. In criminal law, isolate a maniac. In a criminal trial, detain a suspect.

The problem is not so much to recognize security measures, but rather to correctly define the scope and reasons for their application.

Security measures always represent a restriction of human rights and freedoms, which is why their limits must be clearly defined. To do this, it is proposed to use personal, territorial and time approaches, which complement each other. A clear designation of the limits of the validity of security measures by the circle of persons to whom they apply, by the territory in which they operate, and by the time of their validity is necessary not only in order to avoid abuse, but also for the optimal distribution of law enforcement resources.

It is possible to identify typical characteristics of a person who may be a source of increased danger and (or) an object of increased protection (age, citizenship, illness, criminal history), and also to identify typical characteristics of the territory in which the security regime in space should be implemented (state border, closed administrative-territorial entity, zone of counter-terrorism operation). Similarly, rules for the operation of safety measures in space should be developed. To limit the time limits of anti-criminal security sanctions, it is necessary to introduce into the theory of law and into legislation the concept of "criminological limitation periods" and establish after what period of time has passed since the commission of a socially dangerous act, security measures cannot be applied.

The limits of security measures can be limited by a dynamic model of multi-level grounds for security measures, the hierarchy of which consists of: social, regulatory, factual (material) and organizational-legal grounds.

The social basis of security measures creates the need to suppress the harmful influence of a source of increased danger or to protect the object of protection from harmful effects by limiting constitutional rights and personal freedoms. In this case, the harm forcedly caused to a person with an increased danger or to third parties must be less than the harm prevented. The proportionality of harm is carried out according to principles similar to the rules of extreme necessity or necessary defense.

Security measures are always restrictions on constitutional rights and freedoms. Events and actions (not only legal, but also illegal) can act as the actual basis for security measures. For the application of security sanctions, the actual grounds will be socially dangerous acts provided for by federal law. When applying security sanctions, the law enforcer must proceed from the presumption of the absence of a social danger to an individual until this property is expressed in a specific socially dangerous action.

The organizational and legal grounds are acts of application in the form of a sentence, court ruling, decision of a judge, prosecutor or other competent decision, in which security relations are individualized. The identified groups of grounds are important at different stages of the application of security measures: social - for lawmaking, normative and legal - for assignment, and organizational and legal - for the implementation of security measures.

The most important condition for limiting the limits of security measures must be the proper procedure for their appointment and implementation. The more noticeably a measure restricts the rights and freedoms of an individual, the more authoritative the body making the decision on its application should be, and the more guarantees against arbitrariness the procedure for making and executing the decision should provide. An exception is possible only for the application of urgent security measures (counter-terrorism operation).

But even in this case, after the fact, a thorough check of the validity of the application of security measures must be carried out. Parliamentary and judicial control is optimal for such cases. If the procedure for applying security measures contains aspects that limit constitutional rights and freedoms, it should be provided for only in federal law. Resolving procedural issues that infringe on the rights and freedoms of citizens in by-laws is unacceptable.

And finally, a necessary prerequisite for the application of security measures must be a forecast, which, unfortunately, is absent when using this institution both on a global and individual scale.

MAIN STAGES IN THE DEVELOPMENT OF RISK THEORY

The term "risk" has an ancient etymology. In its original literal interpretation, mentioned by Homer, it was characterized as “the danger of maneuvering between rocks.” The Greek term “ridsikon”, the Latin term “ridsicare”, and the French term “risdoe” are associated with this interpretation. The first attempts to understand the concept of risk date back to the 13th century.

This happened thanks to gambling. Gambling has been known since ancient times and developed in different variants. No one tried to calculate the possible number of outcomes. The main reason was that there were no interested parties in such a calculation.

Dice were widely used for casting lots and divination, so any attempt to predict the outcome of a throw could be seen as an attempt to predict the corresponding divine action. The earliest known attempt to calculate the number of possible outcomes of throwing three dice, including permutations, appears in a poem by Richard de Fornival.

In the 16th century, Cardano tried to comprehend the laws of the game. In his treatise, The Book of Random Games, attempts were made to develop the statistical principles of probability theory. He formulated the idea of probability as the ratio of favorable outcomes to the total number of possible ones. At the same time, he himself practically did not use this concept, but used the word “chance”. In the 17th century, Blaise Pascal explored gambling.

In collaboration with Pierre de Fermat, he solved a mathematical problem about the distribution of a bank between two players in the event of the termination of an unfinished game with a clear advantage of one of the players at the end of the game.

The simple solution of dividing the bank equally was rejected by Fermat and Pascal, considering it completely unfair, thus, for the first time, a mathematical solution was associated with a problem of moral law. As a result, Blaise Pascal and Pierre de Fermat developed the theory of probability, which provided new opportunities for assessing the magnitude of risk.

Pascal and Fermat also proposed a systematic method for calculating the probability of future events. This allowed quantitative predictions of the future to be made scientifically. However, the use of the apparatus of probability theory required the presence of probabilities that must be calculated based on the available data.

An ingenious solution to this problem was John Grant's proposal to use sampling in decision making. In 1662 in London, he published Natural and Political Observations Concerning Death Certificates, which pioneered the use of sampling and probability methods, which are the basis of risk management. Later, Edmund Halley, using Grant's scientific approaches, conducted a statistical study in Breslau for the years 1687 - 1691. Having detailed data on fertility and mortality, he obtained unique results: he estimated the total number of people living in a given city.

Halley also conducted a detailed mathematical analysis of the value of different types of rent. Currently, insurance risk management is unthinkable without using the ideas of Grant and Halley. The development of the insurance business had another important direction - marine risk insurance. At the same time, information was needed about new routes, countries and shipping conditions. There was no media at that time, and the main gathering place was coffee shops in port cities where sailors, merchants and insurers gathered.

Edward Lloyd, the owner of a coffee shop on the banks of the Thames, noticed the interest of his customers in certain information and in 1696 began issuing an information sheet that collected information about arriving and departing ships, about the situation abroad and at sea, about shipwrecks. It has become clear that additional information about shipping conditions can significantly reduce risks.

By the end of the first stage of development of scientific knowledge about risk, humanity had learned to determine the amount of risk using the methods of probability theory. However, the issues of taking into account the influence of the subjective factor on the accuracy of risk assessment have not been resolved. In addition, calculating probability based on facts that have already taken place made it difficult to make decisions looking to the future.

In the early 18th century, Gottfried Wilhelm Leibniz proposed the idea and Jacob Bernoulli substantiated the law of large numbers and the basic procedures of statistics. In his work "The Law of Large Numbers," J. Bernoulli showed how, given a limited set of data, one can calculate the probability and statistical significance of events. He was the first to formulate the problem of determining probability based on information about a limited selection of real events; he also proposed the assumption that, under equal conditions, the occurrence or non-occurrence of an event in the future will follow the same patterns as those observed in the past.

In 1738, Daniel Bernoulli, noticing that when choosing a decision, more attention is paid to the consequences of risk than to its probability of occurrence, he proposed the concept of "risk utility", on which the modern theory of portfolio investment is largely built.

The usefulness in each individual case depends on the person making the assessment, since people who find themselves in the same situation, for example, an emergency situation during an airplane flight, behave differently.

In the 18th century, the basic principles of the theory of risk in entrepreneurial activity began to form, associated with the paradigm of economic analysis of classical political economy, primarily with the works of A. Smith. In his book “An Inquiry into the Nature and Causes of the Wealth of Nations” (1784), he examined the theory of entrepreneurial risk using examples of the payment of wage workers, the functioning of lotteries and the practice of insurance.

Characterizing differences in wage levels from the perspective of a risk factor, he argued that workers demand higher pay in cases where permanent employment is not guaranteed. This principle of forming the terms of an employment contract later became the basis of one of the well-known theories, considered as a transaction between a risk-averse employee and a risk-neutral company. A. Smith was one of the first to show that entrepreneurial risk has not only an economic, but also a psychophysical nature, and came to the conclusion that professions with a high level of risk guarantee, on average, higher pay than professions with a low level of risk. This conclusion was later used as the basis for the modern postulate of risk theory - the relationship between the levels of profitability and risk.

At this time, the classical theory connecting the concepts of risk and entrepreneurial profit, which belongs to John Stuart Mill, was formulated. In his book The Principles of Political Economy, Mill views business profit as the sum of the capitalist's wages, the share (interest) of the capital invested, and the risk fee. Risk payment according to Mill is compensation for possible damage associated with the risk of loss of capital as a result of business activity.

Subsequently, John Maurice Clark began to consider risk the only source of entrepreneurial profit. Karl Marx noted the direct dependence of the degree of entrepreneur’s willingness to take risks on the expected profit. Further development of risk theory is associated with the research of J. von Thünen. In his work “The Isolated State in Its Relation to Agriculture and the National Economy”

(1850), he first examined the essence of innovative risks in the process of entrepreneurial activity.

Thünen defined entrepreneurial profit as the income remaining from the gross profit of a business operation after paying interest on invested capital, management fees and insurance premiums on calculated risks of loss. The entrepreneur's remuneration is thus income for taking on those risks that, due to their unpredictability, no insurance company will cover. This finding was the first to highlight the differences between conditions whose probabilities can be calculated and conditions whose probabilities are unpredictable.

In the 20th century, the concept of “risk” was recognized as an integral component of any business activity carried out under conditions of uncertainty. Risk was considered as a result of the impact of anthropogenic artificial and natural factors, which is possible with a high level of human knowledge about the world around us. There is a need for a systematic approach to risk management. Complex assessment and forecasting systems have emerged to effectively manage risks. At the same time, to quantitatively measure the magnitude of risk, the mathematical apparatus of probability theory, using the concept of “randomness,” was widely used.

A certain contribution to the development of innovative risk theory was made by I. Schumpeter. In his book “Theories of Economic Development” (1912), he proposed a new approach to assessing the role of entrepreneurs carrying out innovative activities. He argued that only technological innovation could generate a positive interest rate. Accordingly, an entrepreneur carrying out innovative activities in high-risk conditions is the source of all positive dynamic changes in the economy.

Alfred Marshall and Arthur Pigou developed the so-called “neoclassical” theory of entrepreneurial risk. The essence of this theory comes down to the following. In a market economy, an enterprise operates under conditions of uncertainty, due to which profit is a random and variable value, so the entrepreneur is interested not only in the amount of profit, but also in the range of its probable fluctuations. According to this theory, it turns out that a small but guaranteed profit is more profitable than a large but doubtful one. Hence the conclusion is drawn that it is unprofitable to participate in gambling, lotteries and similar gambling activities.

In 1921, F. Knight, in his book “Risk, Uncertainty and Profit,” developed J. Thunen’s conclusion about the differences between countable and uncountable business risk. He pointed out the need to separate the concepts of risk and uncertainty. Measurable uncertainty is risk. Unmeasurable uncertainty is uncertainty. The theoretical conclusions of F. Knight made it possible for the first time since A. Smith to clearly separate the risk factor from the factors of production in the process of forming business profit.

On the agenda was the development of a theory for choosing a risk-taking option for capital investment (investment), taking into account the risk in lending associated with technological reasons (wear and tear of equipment), natural disasters, price fluctuations and consumer demand. John Maynard Keynes made a significant contribution to solving these problems. He introduced the concept of risk costs, meaning by them those funds that an entrepreneur must include in costs to insure in case of deviation of actual revenue from planned revenue.

Risk costs should include funds to cover possible drops in market prices, accidents and catastrophes, and premature wear and tear of equipment. An entrepreneur must take into account the risk of losing expected benefits from unforeseen circumstances; the lender's risk of possible loan loss; the risk of losing the real value of money over time. Progress in understanding risk and uncertainty has been made within the framework of strategic game theory. In 1953, Neumann, together with Oscar Morgenstern, published the book “Game Theory and Economic Behavior.” Game theory has opened up a fundamentally new approach to understanding the essence of uncertainty.

The source of uncertainty is the intentions of other people. For economic and social problems, games play - or should play - the same role that various geometric and mathematical models successfully play in the physical sciences. One of the most important moments in the development of risk theory was the emergence of the concept of “diversification,” proposed in 1952 by Harry Markowitz. Diversification allows you to minimize investment risk through a thoughtful distribution of investments, for example, when forming an investment portfolio. Markowitz defined the concept of “dispersion (volatility)” as a measure of risk or uncertainty of income.

Daniel Kahneman and Amos Tversky in the 60s of the 20th century studied human behavior under conditions of risk and uncertainty. They developed prospect theory, in which they described stereotypes of human behavior that had not previously been noticed by supporters of the theory of rational decision making. At present, classical and neoclassical theories do not exist in their pure form, since they have undergone a certain transformation.

The generally accepted theory of economic risk now is neoclassical with the additions made by J. Keynes. He was the first to give a detailed classification of entrepreneurial risks, supplementing the neoclassical theory with the factor of pleasure. Keynes considered the main drawback of the previous neoclassical theory to be the underestimation of the propensity for excitement, which is often found in the practice of entrepreneurs.

The further development of the neoclassical risk theory was presented in the works of T. Baczkai and D. Messena, who argue that the essence of risk is not the damage caused by the implementation of a decision, but the possibility of deviation from the goal for which the decision was made. This means that along with the risk of incurring expenses, there is a risk of receiving additional income (profit).

RISK THEORY

Risk in classical theory is identified with the mathematical expectations of losses that may result from the implementation of the chosen decision. The main provision of the classical theory is the definition of risk as the probability of incurring damages and losses from the chosen decision and activity strategy.

This interpretation of risk is one-sided. It entailed the development of another theory, which was called neoclassical. This theory is based on the following provisions: an enterprise (or firm) that operates under conditions of uncertainty and whose profit is a random variable must be guided in its activities by two criteria: the size of the expected profit and the magnitude of its possible fluctuations.

According to this theory, the behavior of an entrepreneur is determined by the concept of the so-called marginal utility. This means that if you need to choose one of two options for investing capital that gives the same business profit, then you should choose the one in which the fluctuations in profit will be smaller. From this theory of risk it follows that a certain profit always has a greater utility than a profit of the same expected size, but associated with possible fluctuations.

The most recognized is the neoclassical theory of risk, but with certain additions made to it by Keynes, who: for the first time systematized the existing theories of risk and gave a detailed classification of business risks; supplemented the neoclassical theory with the “pleasure” factor, which consists in the fact that an entrepreneur, in anticipation of greater profits, is likely to take greater risks. The risk is considered from the point of view of possible material damage associated with the implementation of economic, organizational, technical decisions, accidents, natural disasters, bankruptcy, decrease in the value of shares and monetary units, as well as from the point of view of decision-making related for profit or income.

Firstly, risk is understood as failure, the danger of material and financial losses that may occur as a result of the implementation of the chosen solution. Secondly, risk is identified with perceived success and profit.

Knight was the first to give the most general definition of risk. Risk is a course of action in an unclear, uncertain environment. Risk is a situational characteristic of an activity that may have an uncertain outcome and adverse consequences in case of failure. These definitions relate to a greater extent to the concept of risk as a whole.

THEORY OF ECONOMIC RISKS

Economic risk should be discussed as a decision-making process under conditions of uncertainty, taking into account both economic and political, moral, psychological and other consequences, mainly adverse ones.

Risk situations are situations that do not have a clear outcome or solution, but necessarily require the choice of one of several options.

Economic risk is the activity of economic entities associated with overcoming the uncertainty of a situation of inevitable choice, during which there are opportunities to assess the likelihood of achieving the desired result, failure and deviations from them for all options under consideration.

In the process of economic activity, when making decisions, one should:

1) take into account the degree of probability of achieving the desired result and the probability of deviation from it;

2) try to identify opportunities to implement your decisions in order to prevent adverse consequences.

There are two functions of risk: stimulating and protective. The stimulating function has two aspects: constructive and destructive. The first aspect is manifested in the fact that risk is a catalyst when solving economic problems, especially when making innovative investment decisions. The second aspect is that making and implementing decisions with unreasonable risk leads to adventurism. An adventure is a type of risk that objectively contains a significant probability of impossibility of achieving the intended goal, although the persons making such decisions are not aware of this.

The protective function also has two aspects: historical-genetic and socio-legal. The content of the first aspect is that people are always spontaneously looking for forms and means of protection from possible undesirable consequences. In practice, this is manifested in the creation of insurance and reserve funds, insurance of business risks. The essence of the second aspect lies in the need to introduce categories of legality of risk into economic, labor, and criminal legislation. The risk assessment process includes three stages:

1) identifying possible solutions to the problem;

2) determination of possible economic, political, moral and other consequences, mainly negative, that may occur as a result of the implementation of the decision;

3) the integral side of risk, which in turn consists of two interrelated aspects - qualitative and quantitative.

The main one is the quantitative aspect of risk assessment. It is generally accepted that it is inappropriate to implement decisions that, although they comply with the quantitative parameters of the assessment, do not meet the qualitative parameters of risk. This approach is generally considered technocratic.

There are three main criteria for quantitative risk assessment.

The essence of the first is that decisions chosen in a risk situation should be assessed from the standpoint of the likelihood of achieving the intended result and possible deviation from the goal.

From a mathematical point of view, risk will be equal to the difference between the expected result of an action in the presence of accurate data of the situation and the result that can be achieved if these data are not determined. As a general rule, it is considered inappropriate to make decisions whose risk is measured by a probability of 0.5–0.6 or higher.

From a financial point of view, risk can be of three degrees:

1) acceptable risk associated with loss of profit in case of failure to implement decisions;

2) critical risk associated with the possibility of non-receipt (loss) of revenue or income;

3) catastrophic risk affecting the liquidation of the company’s positions and the possibility of its solvency; such a risk is a direct prerequisite for the bankruptcy of the company.

The second criterion for quantitative risk assessment is that the best solution will be the one that, under existing conditions, ensures the achievement of the desired result at lower costs compared to other options.

The essence of the third criterion is that the best solution will be the one that takes the least amount of time to implement.

The degree of risk is defined as the product of the expected damage and the probability that this damage will occur.

RISK INSURANCE

One of the common reasons for losses and, as a consequence, bankruptcy of enterprises is the risks of non-payment for goods supplied, disrupted deliveries (short deliveries) of products, non-fulfillment of work and services.

Property interests of the insured associated with the risk of losses due to non-fulfillment (improper fulfillment) of their obligations by the insured's counterparties when carrying out business activities for the following types of transactions: purchase and sale, including the supply of goods, supply of goods for government needs, contracting , sale of real estate, sale of enterprise; exchange; rent, including rental, lease of vehicles, buildings or structures, enterprises, financial lease (leasing); contract, including household, construction, contract for design and survey work, contract work for government needs.

The list also includes the implementation of research and development and technological work; paid provision of medical, veterinary, auditing, consulting, information, real estate, tourism and communication services; shipping; transport expedition; storage in a warehouse; commission. It is expected that bank guarantees will be issued; opening a letter of credit; loan; factoring.

Insurance risk is a financial business risk associated with non-fulfillment, improper fulfillment by the insured's counterparty (debtor) of obligations assumed under an agreement with the insured, expressed in: non-delivery, short-delivery of goods, non-transfer of property (goods), non-performance of work, non-provision of services in terms established by the contract; supply of goods of quality and completeness that do not comply with the terms of the concluded contract (only for purchase and sale transactions, supply of goods, supply of goods for government needs); failure to pay money (failure to make payments) within the time limits established by the agreement (including the leasing agreement). Also expressed in the non-return of funds paid by the policyholder under a bank guarantee (surety), if this is provided for in the agreement between the guarantor and the principal (guarantor and debtor).

Expressed in non-return of funds paid by the policyholder under the letter of credit, if this is provided for in the agreement between the applicant and the issuing bank; failure to return funds by the debtor (creditor) provided by the policyholder under the factoring agreement; failure to return funds issued by the policyholder under the loan agreement.

When an insured event occurs, the policyholder must notify the insurer about the event, which can be recognized as an insured event within three days. Depending on the terms of insurance, the procedure and timing for filing an application for an insured event in the prescribed form are agreed with the insurer on the basis of the insurance rules.

ECONOMIC SECURITY OF CORPORATIONS, COMPANIES AND ENTERPRISES

Economic corporate security is a certain characteristic of the state of a company and enterprise, which it is desirable to measure quantitatively either as a scalar or as a vector quantity. The economic security of a business structure presupposes the protection of its vital interests from internal and external threats. This is the protection of the business structure, its human and intellectual potential, information, technology, capital and profit, which is ensured by a system of measures of a special legal, economic, organizational, information, technical and social nature.

The definition of safety should not only be based on the interests of the owner, but also take into account the interests of other interested parties. Due to these circumstances, a more reasonable approach to determining the economic security of an enterprise is from the standpoint of achieving the goals pursued by the enterprise, which indirectly take into account the interests of the parties interested in its activities.

The economic security of an enterprise as an economic object is determined by the state of the architecture, the dynamics of functioning, compliance with vital interests, meeting needs and the development trend. This characteristic is subject to impacts that negatively affect the functioning of the enterprise. This impact is seen as a threat leading to deterioration in performance.

It is assumed that the enterprise has some basic characteristic that may be subject to undesirable effects. If this characteristic is protected from unwanted influences (threats), then the economic security of the enterprise is thereby ensured. The criterion for assessing safety is either absent or assessed by profit. For an enterprise as an economic entity, its mission is always defined, which determines the goals and results of its activities.

Carrying out its activities in the external environment, the enterprise has an architecture that allows it to function on the one hand, and on the other hand, allows it to be in an equilibrium, stable state, which can be called safe.

This means that the management of the enterprise ensures its successful operation and achievement of its goals, despite the negative impact of the external environment. And if the change in external conditions goes beyond certain limits, then management cannot ensure the effective functioning of the enterprise and the achievement of its goals due to the finiteness of its resources and the limitations imposed by the architecture.

The term “economic security” is defined through the concepts of “threat”, “danger”, “undesirable changes”, “unforeseen circumstances”. For practical activities, it is advisable to anticipate the emergence of threats so that planning actions to ensure economic security are truly effective and efficient. However, it does not follow from this that economic security is secondary to the concept of threat. Consequently, the economic security of an enterprise is a characteristic of the state of the enterprise, regardless of the existence of certain threats. This characteristic should change slightly with limited fluctuations in the external environment.

It is always important for the owner, and therefore the management of the enterprise, that the enterprise achieves the desired economic results. It depends, firstly, in what state the enterprise is, secondly, what decisions will be made and implemented, thirdly, what capabilities the enterprise has to implement the decisions made. These aspects concerned mainly the internal environment of the enterprise, which, of course, affects the economic security of the enterprise. But the external environment also directly influences the achievement of planned results, which also implies the implementation of measures for the economic security of the enterprise.

Consequently, if the normal functioning of the enterprise (internal environment) is ensured, and changes in external conditions do not differ greatly from those expected, then the enterprise will achieve its goals and results.

The normal functioning of an enterprise is understood as receiving profit from its activities that meets the owner's expectations. The economic security of an enterprise is such a characteristic of the state of the enterprise in which it is able to achieve its goals and results with limited changes in the external and internal environment.

The limited changes in the two environments only indicate that absolute economic security does not exist. It can only be achieved under certain conditions. For example, in case of abrupt changes in prices for products, raw materials, energy resources, a sudden increase in wages, the unexpected introduction of new legislation, unforeseen sanctions of other states, it is not possible to ensure the economic security of the enterprise if the mentioned actions lead to a sharp decrease in profits, profitability or bankruptcy.

An enterprise is characterized by the presence of an internal environment that determines its state, and an external environment that influences the results of its activities. Thus, there are certain economic conditions, some of which it can influence, but the rest it cannot significantly influence. For example, the economic security of an enterprise cannot be ensured in the event of force majeure circumstances, such as natural disasters, man-made disasters, wars, strikes, revolutions.

Consequently, an assessment of the degree to which planned results and goals are achieved can serve as a criterion for assessing the economic security of an enterprise. In this regard, two components can be distinguished: the state of property and economic decisions on its use. For an enterprise, its condition is determined by the architecture and the availability of such components necessary for the production.

Analysis of points of view on the economic security of the enterprise as raw materials, energy resources. The state of the external environment is determined by the amount of demand for the enterprise's products and the price parameters of the components listed above. The performance of an enterprise is determined by the income that the owner receives from its activities in the form of dividends and partners (payments for supplied materials, components, energy resources); clients (trade of enterprise products); personnel (remuneration for labor); state (taxes). If the amount of income is sufficient according to the views of the above parties in the present and future, then we can talk about sufficient economic security of the enterprise.

Thus, the way to achieve a state of economic security of an enterprise is determined by the timely fulfillment of obligations in the present and future with possible changes in operating conditions. Preservation of property is necessary, and its effective use is a sufficient condition for the economic security of the enterprise. On this basis, the planned results are set; the functions, powers and degree of responsibility of management are determined; investments are directed and the necessary resources are allocated; costs are controlled.

The main controller at the enterprise is the accounting department, the purpose of which is to maintain the integrity and ensure the correctness of settlements with suppliers, clients, owners, staff and the state. Ensuring the economic security of an enterprise lies in the adoption and implementation of management decisions that maximize the income of all interested parties, subject to the preservation of property in the present and future.

The main ones in this case are all services that ensure the innovative development of the enterprise. Innovation is a necessary condition for maintaining the competitiveness of an enterprise and determines its investment policy, the purpose of which is to increase property value.

Increasing value involves changing the enterprise architecture in such a way that the efficiency of using property increases or at least does not decrease (in the event of an unfavorable state of the external environment). Thus, an approach based on combating threats must be obviously lower in effectiveness than an approach based on preserving property and the efficiency of its use.

THE CONCEPT

The concept of economic security of an enterprise is closely associated with the threats that arise in the course of its activities. Currently, in the literature there are many definitions of the terms: “threat to economic security”, “threat to business security”, “threat to enterprise security”, which can be interpreted in different ways, or can be perceived as synonyms.

If we rank the terms, then the first place should be given to the term “threat to economic security”, which determines the negative impact on any economic activity, for example, very high inflation rates. “Threat to business security” implies the creation of conditions under which it is impossible to create new or diversify existing enterprises, which may be reflected in the state’s monetary policy or in the Tax Code.

A threat to the security of an enterprise may consist in the emergence of conditions under which current activities in any industry or even a specific enterprise are difficult. The term “threat” refers to any conflict of goals with the external environment or internal structure and functioning algorithms.

The first point of view does not directly connect the threat with damage, but only reveals contradictions between the goals and possibilities of achieving them, on the one hand, and the state of the external environment and enterprise architecture, on the other.

The result is the determination of achievable goals, the choice of adequate means of their implementation in the event of a discrepancy between these goals of the internal structure, which needs constant transformation, and the dynamic external environment. Therefore, planning is a process that is aimed at eliminating these inconsistencies.

The market is a permanent conflict, including between producers. Therefore, an enterprise always has some restrictions that must be taken into account when planning its activities. These are not only restrictions on sales opportunities, available resources and markets, legislative restrictions, restrictions, but also those dictated by competition.

When planning to achieve the goals of your activities, it is necessary to take into account the reality of their achievement, which is not always possible due to the subjective point of view on the possibilities of their implementation. The possibility of implementing any plan is probabilistic. They have one degree or another of risk. Both from the point of view of assessing existing restrictions on activity, and from the point of view of taking into account the uncertainty of the future, there is always a risk of incurring losses, both in the form of lost financial profits and real ones, which is considered a threat to economic security.

It is positive to state the fact that architecture and management actions themselves can pose a threat to the enterprise. Thus, we can come to the understanding that management decisions made and implemented by management can also pose a threat to the enterprise. The second point of view determines the result of the threat, since it records its presence only after damage has been caused to the enterprise.

The third point of view notes that a threat does not necessarily lead to consequences in the form of disruption of the functioning of the enterprise and causing damage. The fourth point of view only adds the probabilistic nature of the threat, without essentially changing the approach.

By threat it is proposed to understand the possibility of an adverse impact on the state or results of the enterprise. Once quantified, a threat can be considered a risk. Consequently, risk is a quantitative assessment of a threat, in turn, a threat is a qualitative definition of risk.

Risk characterizes the uncertainty of conditions and results of activities, and a threat is the possibility of negative developments. It is necessary to distinguish the situation of threat and risk from their implementation. The realization of a threat is a risk that has begun to materialize according to an undesirable option or a previously known scenario for an unfavorable development of events, respectively, going beyond the scope of the uncertainty of operating conditions envisaged by planning.

Economic security is characterized by a system of protecting economic interests from unfavorable macroeconomic factors, destructive behavior of owners, partners or competitors.

Economic security ensured by legitimate methods is characterized by a system of methods for protecting the economic interests of an enterprise that are fully consistent with current legislation. Economic security ensured by illegitimate methods is characterized by a system of methods for protecting the economic interests of an enterprise from threats that contradict current legal norms.

The main thing in ensuring the economic security of an enterprise is the preservation of property. The main part of economic security research from this point of view is devoted to identifying and preventing violations of legislation in enterprise management.

At the same time, it is believed that economic security can be ensured by a separate structural unit - the security service. Therefore, the main attention is focused on describing the structures and functions of security services, security systems, as well as integrated approaches to the problem thus formulated. This approach has practical usefulness, especially insofar as it concerns methodological recommendations that can be implemented.

Enterprise management is also considered the main focus. The degree of achievement of goals is used as a criterion. If the set goals are not achieved, it is considered that the economic security of the enterprise is not ensured. The state of economic security of an enterprise is assessed from the standpoint of its competitiveness; strategic sustainability; financial stability.

The actions of the security service cannot ensure it. This follows from the fact that this service is subordinate to the first person of the enterprise (director), who has to make economic decisions that carry one or another risk of loss. And the security service cannot prevent this.

The main functions performed by this service relate to monitoring the actions of personnel in terms of compliance with the law, the operating mode of the enterprise, the protection of material and technical assets, intellectual property and intangible assets. But this is clearly not enough to ensure the economic security of the enterprise in the broad sense.

In practice, the boundaries of an enterprise and a legal entity may not coincide. From the point of view of the owner and manager, the financial and economic activities of an enterprise are understood as the activities of the enterprise, its divisions and employees in relationships with the external environment and among themselves, leading or potentially capable of leading to a change in the assets and liabilities of the enterprise, i.e. property. During the operation of the enterprise, economic relations with the owner, staff, state, partners and clients are constantly maintained.

THE DANGERS OF THE SHADOW ECONOMY

Legal regulation of economic security processes includes a system of conditions established by legal norms that establish the procedure for actions of business entities and economic relations between them, aimed at achieving their goals. At its core, economic security is one of the forms of manifestation of the general desire of business entities for stability and reliability on the principles of freedom, defined by the relevant laws, which concentrate the interests of the individual, the collective, and the state.

These two aspects of legal support for economic security are closely interconnected, since the content of any law is to determine the rights and obligations of individuals and legal entities under conditions of coercion, accompanied by features emanating from the economic interests of the state and society based on the principles of law.

The principles of law to ensure economic security are reflected in its norms and are the basis for the legal support for the organization and activities of business entities. Legal principles directly related to the problem of ensuring economic security include:

- universal obligatory compliance by the entire population of the state with the rules of law;
- absence of inconsistency in the rules of law that make up the system for ensuring economic security;
- compliance of objective norms of law with subjective ones, as well as norms of law with legal relations;
- division at the legislative level of rights into its types (public and private);
- equality before the law and court of all persons without exception;
- responsibility and conditionality of the behavior of individuals and legal entities within the framework defined by laws;
- justice, expressed in equal legal responsibility and proportionality to committed offenses;
- the humanity of punishment, which contributes to the correction of convicts.

Although economic security has gained new importance in the global economy, it is inextricably linked to indicators such as economic growth, stability of the socio-economic system, government revenues, tax base, government debt and inflation, and unemployment.

Economic growth cannot be sustainable without the dynamic development of the economies of other countries. Until the economy develops, there will be no adequate response to external and internal threats. The ability of the economy to survive in difficult situations will remain abstract.

A system of indicators for assessing the level of economic security and determining their standard values is important in state economic policy. Indicators of the level of economic security of the country and their threshold values are approved at the government level.

The state of economic security is assessed by a system of objective criteria and indicators that determine the maximum dimensions of the functioning of the economic system. When these dimensions are exceeded, the system loses the ability to develop dynamically, becomes uncompetitive in external and internal markets, becomes the object of expansion of transnational corporations, the country's national wealth is plundered both within the country and abroad, and it suffers from corruption.

The economic security of the state is influenced by the volume of the shadow economy. The shadow economy can be characterized by its scale and its destructive role. The growth of the shadow economy leads to a reduction in government revenues by reducing the tax base. This, in turn, leads to a decrease in the quality of socio-economic conditions in general.

The shadow economy is a certain economic activity that is carried out on the territory of the state for the purpose of tax evasion and is not officially taken into account. Therefore, its development has a negative impact on the socio-economic situation. The study of the causes of the emergence and development of the shadow economy in society began in the last century.

Because the share of the shadow economy in the production of goods and services provided increased during this period.

Practice has proven that there are two interrelated particular aspects of the shadow economy:

- commit illegal actions in order to obtain uncontrolled personal income;
- hide from control all or part of the income received as a result of activities in order to obtain additional personal income.

Regardless of the degree of economic development, the existence of such situations causes an increase in the number of negative socio-economic consequences in society.

The shadow economy is a complex phenomenon characteristic of all countries of the world. According to the World Bank, the global average level of the shadow economy is 17.2% of GDP. Economic policy based on incorrect economic statistics has a negative impact on the stability of economic development. And the results of the development of international institutions for coordinating economic policy, which is a contributing factor in the functioning of the modern world economy, may also turn out to be ineffective.

Today, more than ever, transparency and legality of transactions in national financial systems are of great importance. For this reason, it is extremely important to create effective mechanisms to combat the shadow economy and corruption in order not only to protect the performance of the country's financial system, but also to ensure the proper use of public funds. In this context, the tasks are set

Expand the use of third-party data and Big Data to identify unregistered taxpayers and transactions. To increase the efficiency of tax control, create contactless centers for the exchange of information between the tax authority, citizens and businesses. Expand the ability of data centers in tax and customs authorities to obtain information about transactions.

DIGITAL ECONOMY

The term "digital economy", introduced by D. Tapscott and disseminated thanks to the scientific research of N. Negroponte, has now become widespread, including due to its practical implementation in the business space of Deloitte and IBM. The digital economy, from the perspective of economic science, can be presented as a certain type of economic relations that arise in the process of production, distribution, exchange or consumption, which acquire a technological character through the use of information, communication and Internet technologies that contribute to the creation of a virtual environment that complements reality.

In the middle of the 20th century, digital technologies were understood as technologies in which information is converted into an intermittent discrete data set consisting of 0 (no signal) and 1 (there is a signal). They were contrasted with analog technologies, where data is a continuous stream of electrical rhythms of different amplitudes with an unlimited number of values. This was later replaced by another definition. Digital technologies are technologies where information is presented in a universal digital form. Another option is all the technologies that make it possible to create, store and distribute data.

In analog technologies, information is not unified. It is stored and transmitted in different formats, for each type of media. For example, a landline telephone is an analog technology, but a smartphone with the Internet is already digital technology. Digital technologies include everything that is associated with electronic calculations and data conversion: gadgets, electronic devices, technologies, programs.

Compared to analog technologies, digital technologies are better suited for storing and transmitting large amounts of data. They provide high computing speed. In this case, information is transmitted as accurately as possible, without distortion. Among the main disadvantages are high energy consumption and negative impact on the climate.

Data centers account for about 0.3% of global carbon emissions. They consume about 200 TWh per year - more than the annual energy consumption of developing countries. By 2030, this figure could rise to 20% of total global demand, leading to a significant increase in emissions.

Digital technologies are often confused with information technology. Information technologies include technologies related to the exchange of information using analog devices. Almost any business uses CRM, online services for remote work, storage and work with the client base, accounting management and inventory accounting. More and more companies are using big data and analytics based on it to develop their business and increase their customer base.

In education, gadgets and programs are used for distance learning, preparing and completing homework, making presentations, programming and creative tasks. Virtual and augmented reality help to better perceive the material and make learning more interactive. AI algorithms help with career guidance and the educational process.

In medicine, digital technologies help to quickly find new drugs and vaccines, make diagnoses more accurately even in the early stages, collect analytics to predict diseases, conduct online consultations and even operations using AR and robots.

In retail, digital technologies simplify the process of searching and ordering goods, managing warehouses and delivery. Analysis of customer behavior and data on movement across sales floors help optimize store space. Voice assistants and chatbots process requests at maximum speed, and offline stores are already starting to operate without cash registers and sales assistants - using cameras and facial recognition algorithms.

In the entertainment segment, digital technologies open up unlimited opportunities for playing games, buying and reading books, listening to music and watching Full HD videos online on streaming services. Neural networks are involved in the creation of music, paintings and books, and virtual actors and musicians replace real actors.

In production, technology is used to automate individual lines and entire plants, develop new models and materials, monitor safety and the environment, predict equipment failures, prevent defects and injuries, and optimize working time and resources.

Digital technologies are involved in collecting and distributing orders, preparing dishes, monitoring the quantity and shelf life of products, and even helping to find new points with maximum traffic.

Some of the most significant digital technologies include deep learning, convolutional neural networks, computer vision, reinforcement learning, natural language processing, recurrent neural networks, transfer learning, generative adversarial networks, decision support systems, smart contracts and speech recognition. Most technologies are related to artificial intelligence, neural networks and machine learning.

Smartphones have combined a personal computer and a telephone, becoming a container for dozens of digital technologies. The Internet of Things is a technology that allows you to connect sensors, gadgets, household appliances and even cars into a single network using wireless communications. All of these devices can be controlled using applications and combined in a variety of automated scenarios - for example, controlling factory equipment. A new wireless communication standard, 5G, opens up great prospects for IoT. With its help, data can be transferred faster, without failures and with minimal delays, connecting even more devices. 5G provides mobile broadband at high speeds and with minimal signal latency of only 1–2 ms.

Most often, “artificial intelligence” refers to any algorithms that solve any problems independently of a person: they perform complex calculations, recognize images and speech, collect and process data sets. But real “artificial intelligence” is one that not only solves problems itself, but also poses new ones, makes decisions itself and goes beyond its original capabilities. In order for AI to act independently, machine and deep learning algorithms are used, and neural networks are constructed by analogy with the neuron systems in the human brain. AI finds the right information, recommends suitable products or videos, builds analytical forecasts, helps treat patients and control drones.

Game developers and marketers were the first to appreciate the capabilities of AR and VR. The former used virtual reality to achieve the effect of complete immersion in a game or virtual tour, while the latter used it to invite customers to “try on” clothes or furniture. In education, a virtual environment helps to visually study anatomy, architecture or ancient civilizations.

In medicine, using augmented and mixed realities, online consultations and operations are carried out. With the help of VR you can visit other countries and attractions, museums and even sunken ships. During the pandemic, developments that allow meetings to be held in AR and VR have become in demand.

3D printing has the potential to replace most manufacturing technologies and materials. 3D printers are used to print parts and spare parts, cables, furniture and fittings, clothing and shoes, and even houses. Bioprinting technology is popular in medicine. When using 3D printers, human tissues and organs are printed from a special biogel.

The first prototypes of robotic devices appeared in the 19th century, and in the second half of the 20th century, robotization reached an industrial level. Robots are used for assembling cars and electronics, logistics, courier delivery, cooking and even surgical operations.

Cloud technologies are based on distributed network access to IT infrastructure to store and process data of any volume. Typically, these are remote servers or IT services that can be rented as needed. This approach allows companies to quickly increase computing power and launch or scale online projects that require very large resources. There are three types of cloud services: IaaS, infrastructure as a service.

When users rent servers, processors and other devices for storing and processing data, they can install their own OS and data processing software on them. The provider provides an OS on which users can install their applications and launch new services. SaaS, software as a service - software as a service.

The user gets access to all provider applications for storing, processing and transmitting data.

Block chain is a technology in which data on all transactions performed is stored in a single system in the form of separate blocks and certified by a digital signature that protects against hacking. The database in the system is distributed among all participants, that is, without any centralized management and control. This makes it, according to its creators, the most independent, safe and resistant to corruption.

Block chain uses tokens–non-fungible, unique entities–as well as smart contracts–algorithms to generate, control, and provide information about ownership of something (for example, crypto currency). The first block was generated in 2009. There are more than 2 thousand different block chain systems. One of the latest modifications is NFT technology, which is used to sell works of art, music tracks and other types of intellectual property. Each image, video or audio is assigned a unique digital certificate that you can purchase to take ownership of the work. NFTs can be resold for profit just like physical art.

Crypto currency is a completely digital currency created using block chain technology, which is used for virtual exchange and payments. It does not depend on banks or other financial institutions. To protect it, exchange and control operations, special encryption methods are used. Block chain technologies in the near future may lead to the emergence of a completely autonomous financial system that will not depend on state and international financial institutions. Perhaps something like a digital state or virtual universe will emerge, with its own internal markets and laws.

The coming years are a turning point in digital transformation, when digital technologies will cover even those areas where analog technologies have always dominated. Government, financial, and medical services are moving to an online format, the first prototypes of electronic passports and digital payment systems are appearing without reference to physical currencies and banks.

The synergy of digital technologies will help unite offline and online, making all devices and services interconnected. Artificial intelligence and big data help you make more informed decisions while VR and AR help you conduct complex operations, travel and learn anywhere.

Assessing the scale of digitalization, researchers come to the conclusion that the digital economy can be considered as a rapidly developing segment of the economic system, in which traditional economic relations and business process management models are replaced and supplemented by new electronic technologies of production, exchange and consumption.

Technical, technological, digital and socio-economic development of society generates new threats and risks. Therefore, issues of ensuring economic security are becoming more acute and vitally important, requiring close study from a scientific point of view.

The economic security methodology makes it possible to identify risks with differences in their acceptable levels depending on controllability and predictability, as well as the possible consequences of their occurrence. This allows us to consider the category of “economic security” as a manageable risk for those subjects who make decisions. In the context of intensive development of information systems and technological solutions, underdeveloped institutions can become a significant factor in restraining the pace of digital development and create conditions for the emergence of new economic security risks.

The basis of the digital economy as a new system of economic relations is made up of tools for the digitalization of economic activity, information and communication services and technologies, end-to-end digital tools, physical and augmented reality technologies, P2P networks, as well as virtual mechanisms in the financial sector.

The action of these tools and technologies influences traditional economic cycles, changing the sequence and nature of production processes and creating conditions for creating added value through the generation of digital economic benefits.

INSTITUTIONAL INFRASTRUCTURE OF THE DIGITAL ECONOMY

The digital economy, like any other type of economic relations, is based on a system of formal and informal institutions that make it possible to make technological decisions and build the rules of the game in new economic conditions. Institutional theory proves that institutions are able to quickly respond to any changes in the system of social relations. New institutions of the digital society may also be formed if systemic changes occur that require transformations.

D. North pointed out that new institutions arise when society feels the need to increase income, but the existing institutional system is unable to provide this. Any institutional change imposes new restrictions on each participant in the relationship. New problems of the institutional environment and new emerging restrictions in the context of digitalization have arisen.

This is

1) the attitude towards the monopolistic effects of platforms and hierarchies: the ineffectiveness of the regulator’s fight against the establishment of monopoly power of platforms, the need for its reorientation to eliminate emerging market failures;

2) changing the rules for regulating digital companies in the direction of replacing licenses with ex post regulation or self-regulation;

3) due to the negative impact of the state standardization system on the number of patents, there is a need to build a new standardization system, taking into account the opinions of independent market players and self-regulatory organizations. In turn, changing restrictions causes a transformation of priorities and a revision of the value of carrying out a particular activity.

For example, in the usual Williamson-McNeil contract model, classical (transactions), neoclassical (cooperation with an intermediary) and relational contracts (firms) are distinguished. In this case, the nature of the assets is the main factor in choosing the type of contracts. Along with this, in the context of digitalization, new types of contracts are emerging, such as: product life cycle contracts based on sharing, smart contracts with the exception of an arbitrator, globalized outsourcing contracts for the "self-employed".

That is why the priorities of business entities will shift towards concluding new types of contracts and increasing demand for new types of contract protection (for example, protection of intellectual property in connection with digital piracy, protection of personal information).

Thus, in the context of the emergence of a digital economy, the adequacy and adaptability of formal and informal institutions will determine the occurrence of positive or negative effects of digitalization. The positive effects of digitalization can be divided into technological, economic and social effects.

This could be a new digital business model, which, thanks to the use of information technology, is capable of scaling on a global scale and covering individuals, business entities and objects of their interaction (goods and services) through effective personal service.

The positive economic effects of digitalization include: expansion of trade markets and operations; increasing labor productivity by reducing costs in various sectors of the economy; development of competition; increasing the number of jobs in related industries; improving the quality of services. The development of the digital economy in the presence of a favorable institutional environment stimulates economic growth and creates conditions for accelerating its pace.

The tools that the digital economy operates allow companies to respond flexibly to changing market conditions and to satisfy emerging consumer needs better and faster. The development of electronic payment systems contributes to a manifold acceleration of the movement of financial flows and is a source of stimulation for international trade exchange.

Traditional companies are moving online and are increasingly using e-commerce tools, thereby accelerating economic development.

The positive social effects of digitalization are also obvious: increasing inclusiveness and reducing poverty; increasing accessibility and improving the quality of medical care; reducing the cost and increasing accessibility of mass education; improvement of the environmental situation; increasing the accessibility of financial services; reducing crime rates; reducing working hours and increasing leisure time for workers. Workers in the 10 most competitive GCI 4.0 economies work on average 361 hours less per year than in the 10 lowest-ranked countries for which working time data exist.

The meaning of digital transformation is to radically reduce the level of transaction costs and change their structure. It is this fact that ensures the success of many digital companies and projects from companies in the sharing economy sector to private blockchain chains. This is due to a significant reduction in the costs of collecting and processing information. However, a dramatic reduction in transaction costs contributes to the expansion of exchange options and causes the emergence of new discrete institutional alternatives. As a result, a “superposition effect” is formed: a simultaneous increase in opportunities and the emergence of development conflicts.

The costs of each group of subjects start to rise due to excessive institutional burden, and regulatory arbitrage also arises, that is, the regulation of similar types of economic activities with varying degrees of intensity. These patterns lead to a flow of business structures into areas of economic activity with a lower regulatory burden.

This situation may arise in conditions of institutional immaturity in the lending market between banking structures and microcredit organizations. This causes a reduction in the scale of the institutionalized market, a fall in effective demand, a decrease in revenue, a massive exit from the market of “players” (with unfulfilled obligations), as well as strengthening of supervision and control measures on the part of the regulator (the effect of a general increase in the regulatory burden).

The emergence of regulatory arbitrage has a direct impact on the consumer, weakening their security and forcing them to reconsider their risk priorities and how they protect and manage them.

CYBER CRIME AND SOCIAL ENGINEERING

One of the negative effects of digitalization has been the intensive development of cyber crime, the economic damage from which has a significant growth dynamics. According to 2017 statistics, more than 130 large-scale targeted breaches occur annually in the United States, and this number is growing at 27% per year. 31% of organizations experienced cyber attacks on their operational technology infrastructure. In 2017, 100,000 groups in 150 countries and more than 400,000 machines were infected with the Wannacry virus.

The total cost of damage was about $4 billion. Crypto jacking attacks increased by 8,500% in 2017. About 24,000 malicious mobile applications are blocked every day.

Social engineering or “attack on a person” is a set of psychological and sociological techniques, methods and technologies that allow one to obtain confidential information. Cybernetic fraudsters who use these techniques in practice are called social engineers. Trying to find access to a system or valuable data, they use the most vulnerable link - the person.

The simplest example is a telephone call, where an attacker impersonates someone else, trying to find out confidential information from the subscriber, playing on the person’s feelings, deceiving or blackmailing him. Many people trustingly tell social hackers everything they need. And scammers have many techniques and tricks in their arsenal.

Social engineering has acquired a strong connection with cybercrime. In the early 70s of the twentieth century, telephone hooligans began to appear, disturbing the peace of citizens simply for the sake of a joke. But someone realized that this way you can get important information quite easily. And by the end of the 70s, former telephone hooligans turned into professional social engineers (they began to be called singers), capable of masterfully manipulating people, determining their complexes and fears by just intonation.

When computers appeared, most engineers changed their profile to become social hackers, and the terms "social engineering" and "social hackers" became synonymous. An example is the theft of $40 million from The Ubiquiti Networks in 2015. No one hacked operating systems or stole data—the employees themselves violated the security rules. The scammers sent an email in the name of a company executive and asked financiers to transfer a large amount of money to a specified bank account.

In 2007, one of the most expensive security systems in the world was hacked - without violence, without weapons, without electronic devices. The attacker took $28 million worth of diamonds from the Belgian bank ABN AMRO thanks to his charm. Fraudster Carlos Hector Flomenbaum, a man with an Argentine passport stolen in Israel, gained the trust of bank employees a year before the incident. He pretended to be a businessman and gave gifts. One day, employees gave him access to a secret vault of precious stones valued at 120,000 carats.

Examples of social engineering show that it easily adapts to any conditions and to any environment. By playing on a person's personal qualities or lack of professional ones (lack of knowledge, ignoring instructions, and so on), cybercriminals literally "hack" a person. An attack on a person can be carried out in many scenarios, but there are several of the most common techniques used by attackers.

Phishing takes advantage of inattention. The victim receives a fake email from some well-known organization asking them to follow a link and log in. To instill more trust, scammers come up with serious reasons for clicking on a link:

for example, they ask the victim to update the password or enter some information (full name, phone number, bank card, and even CVV code!).

Trojan technology exploits people's feelings of greed. It is not for nothing that the virus got its name based on the principle of operation of the Trojan horse from the ancient Greek myth. The only bait here is an email message that promises quick profits and winnings. As a result, a person receives a virus, with the help of which attackers steal his data.

Technology “quid pro quo”, from the Latin “quid pro quo” using this method, the attacker poses as a technical support employee and offers to fix problems with the system, although in fact there were no problems with the software. The victim believes in the presence of malfunctions and, following the instructions of the hacker, personally gives him access to important information.

Another technique that cyber criminals resort to is called pretexting. This is an action worked out according to a pre-drawn up scenario. To obtain information, the criminal impersonates a person known to the victim who allegedly needs confidential information to perform an important task.

Social engineers introduce themselves as employees of banks, credit services, technical support, friends and family members. For greater reliability, they provide the potential victim with some information about her: name, bank account number, the real problem with which she contacted this service earlier. An example is black “call centers”, when prisoners disguised as employees of large banks call citizens and trick them into transferring money.

The reverse social engineering technique is aimed at ensuring that the victim himself turns to the social engineer and gives him the necessary information. This can be achieved through the implementation of special software. At first, the program or system works properly, but then a failure occurs, requiring specialist intervention.

The situation is set up in such a way that the specialist to whom they turn for help turns out to be a social hacker. By adjusting the operation of the software, the fraudster performs the necessary manipulations for hacking. And when the hack is discovered, the social engineer remains above suspicion.

Attackers may advertise their services as computer technicians or other specialists. The victim contacts the hacker himself, and the criminal not only works technically, but also extracts information through communication with his client. If you do not want to become another victim of social engineers, we recommend that you follow the following protection rules.

Always pay attention to the sender of the letters and the address of the site where you are going to enter some personal data. If this is mail on the domain of a large organization, make sure that the domain is exactly that and there are no typos if in doubt contact technical support or a representative of the organization through official channels.

Do not work with important information in front of strangers. Fraudsters can use so-called shoulder surfing - a type of social engineering when information is stolen over the victim's shoulder - by peeping. Do not go to suspicious sites or download dubious files.

After all, one of the best assistants of social engineering is curiosity. Do not use the same password to access external and corporate work resources. Install an antivirus. All major antiviruses have built-in scanning for malicious resources. Read the company's privacy policy. All employees should be instructed on how to behave with visitors and what to do if illegal entry is detected.

DOXXING

Doxing is an abbreviation for the English slang words “drop drop dox” (drop documents), “dox” (documents). Typically, doxxing is a malicious act directed at people with whom the attacker disagrees or is not on the best terms.

Doxxing is the act of disclosing identifying information about someone online, such as their real name, home address, place of work, phone number, financial information, and other personal information. This information is subsequently disseminated without the victim's permission.

Although the disclosure of personal information without the owner's permission occurred before the advent of the Internet, the term doxxing first appeared in the hacker subculture in the 90s of the twentieth century, where anonymity was considered sacred.

Nowadays, the use of the term “doxxing” has expanded beyond the hacker community and is used to describe the fact of the disclosure of personal information. While the term is still used to describe the exposure of anonymous users, it has become less relevant as most use their real names on social media.

Lately, doxxing has become a tool in culture wars, with rival hackers exposing those who hold opposing views. The goal of doxxing is to take the conflict from the Internet into the real world by revealing information that includes: home addresses; information about the place of work; personal phone numbers; social security numbers; bank account and credit card information; details of personal correspondence; criminal history information; Personal Photos; compromising personal data.

Doxxing attacks range from fake newsletter sign-ups or pizza delivery to family stalking, identity theft, threats and personal harassment.

Politicians and journalists are often doxxed. They suffer from online harassment, fearing for their safety and sometimes even their lives. This practice has also spread to executives of large companies. Doxxing became widely known in December 2011, when the professional hacker group Anonymous revealed detailed information about 7,000 law enforcement officers in response to an investigation into hacking activities. Since then, Anonymous has exposed hundreds of alleged KKK (Ku Klux Klan) members, with one of their latest targets being Q-Anon supporters.

The motives for doxxing vary. Individuals who have been attacked or insulted desire revenge. The attack may be aimed at those with an opposing point of view. However, this tends to be the case when it comes to particularly sensitive issues rather than everyday political disagreements.

Intentional disclosure of personal information online usually occurs with the intent to punish, intimidate, or humiliate the victim. However, doxxers may also view their actions as a way to punish someone for past mistakes, hold someone accountable in the public eye, or reveal plans that have not previously been revealed publicly.

Regardless of the motivation, the main purpose of doxxing is to violate privacy and make people uncomfortable, sometimes with dire consequences. There is a huge amount of personal information available online, and people often have much less control over it than they realize. This means that anyone with the time, motivation and interest can turn this data into a weapon.

Many people use the same username on different services. This allows potential doxxers to get an idea of the victim's interests and how they spend their time online. Information about each domain name owner is stored in a registry, which is often publicly accessible using a WHOIS lookup. Let's assume that the person who purchased the domain name did not hide personal information when purchasing. In this case, his personally identifiable information (name, address, telephone number, place of work and email address) is available to everyone on the Internet.

If someone uses an unsecured email account, then attackers can expose that person's confidential emails and publish them online.

If social media accounts are public, anyone can find out the information and initiate cyber stalking. You can find out your location, place of work, information about friends, get photos, see likes and dislikes, places visited, find out the names of family members and pets. Using this information, doxxers can even find answers to security questions and hack other accounts.

Doxxers may use various methods to determine the IP address associated with a physical location. Once they know the IP address, they can use social engineering techniques on the ISP and get more information about the victim. For example, they may file a complaint against the owner of the IP address or try to hack the network.

By finding out a mobile phone number, attackers will be able to obtain more information about a person. For example, search services by phone number, such as White pages, allow you to determine the identity of the owner of this number using a mobile or any other phone number.

Sites like White pages only provide city and state data for free. They charge a fee for providing additional information related to the mobile number. For a fee, you can find out additional personal information about a person using their mobile phone number.

The term "wiretapping" is sometimes used in connection with doxxing. It is used in connection with doxxers who intercept data on the Internet, looking for everything from passwords, credit card numbers and bank account information to old email messages. Doxxers connect to a network, break its security, and then collect data going in and out of the network. One way to protect yourself from network eavesdropping is to use a VPN.

Data brokers exist to collect information about people and sell that information for profit. Data brokers collect information from public sources, loyalty cards (which track online and offline purchases), internet search history (everything users searched for, read, and downloaded) and other data brokers. Many data brokers sell information to advertisers, but some people search sites offer comprehensive records of people for a relatively small fee. The doxxer only needs to pay the required amount and obtain the necessary information to begin pursuing the victim.

By collecting information scattered across the Internet, doxxers can create a picture that will lead to the discovery of the identity of the real person hiding behind the pseudonym: his name, residential address, email address, phone number and much more. Doxxers can also buy and sell personal information on the dark web.

The information found can be used as a threat, for example, posted on Twitter in response to an opponent's disagreement. Doxxing may not be so much about the disclosure of information as it is about how it is used to intimidate or harass the victim. For example, someone who has your address can find you or your family. Someone who has your cell phone number or email address may bombard you with messages that prevent you from communicating with customer support. Finally, by knowing your name, date of birth, and social security number, an attacker could hack into your accounts or use your personal data for their own purposes.

Anyone with the will, time, internet access and motivation can put together a dossier on the victim. And if the victim of doxxing has ensured the relative availability of data about himself on the Internet, it will not be at all difficult to steal it. The most common types of doxxing can be divided into three categories: publishing personal, personally identifiable information online; disclosure on the Internet of previously unknown information about a private person.

Disclosure of information about individuals on the Internet may damage their reputation and the reputation of their partners. Doxxing can destroy lives because doxxing can expose both victims and their families to harassment, both online and in the real world. Doxxing is not illegal if the information disclosed is in the public domain and was obtained through legal means. However, depending on the jurisdiction, doxxing may run afoul of laws designed to combat stalking, harassment, and threats.

It also depends on the type of information disclosed. For example, revealing someone's real name is not considered as serious as disclosing a home address or telephone number. However, in the United States, disclosing information about a government employee is subject to federal conspiracy laws and is considered a federal offense. Since doxxing is a relatively recent phenomenon, the laws surrounding it are constantly changing and are not always clear.

Regardless of laws, doxxing violates the terms of use of many websites and can therefore result in banning. This is because doxxing is generally considered unethical. In most cases, it is carried out with malicious intent to intimidate, blackmail and control others.

Victims of doxxing are subject to potential harassment, identity theft, humiliation, job loss, and rejection from family and friends. Using antivirus software can prevent information from being stolen using malicious applications. Regularly updating your software helps prevent security holes that can lead to hacking and information disclosure.

A strong password usually consists of a combination of uppercase and lowercase letters, as well as numbers and symbols. Avoid using the same password for multiple accounts and change your passwords regularly. If you have trouble remembering passwords, use a password manager.

If you use online forums such as Reddit, 4Chan, Discord, YouTube and others, make sure you use different usernames and passwords for each service. If you use the same name, doxxers will be able to identify your comments on different platforms and use this information to build a detailed picture of you. Using different usernames for different purposes will make it difficult for your activity to be tracked across different sites.

Consider using different email accounts for different purposes: professional, personal, and spam. A personal email address can be used to correspond with close friends, family members and other trusted persons; Avoid using this address publicly. A spam email address can be used to sign up for accounts for various services and promotions.

Your work email address (whether you are a freelancer or an employee) can be listed publicly. As with public social media accounts, avoid putting too much identifying information in your email address (avoid addresses like firstname.lastname.date of birth@gmail.com).

Evaluate the privacy settings of your social media profiles and make sure you are comfortable with what information about you is shared and with whom.

Determine which platforms you use for what purposes. If you use the platform for personal purposes (for example, sharing photos with friends and family on Facebook or Instagram), increase your privacy settings. If you use the platform for professional purposes (such as keeping up with the latest news or posting links to your work on Twitter), you can leave your profile public. In this case, avoid posting sensitive personal information and images.

You or anyone trying to log into your account will need at least two forms of identification: typically your account password and your phone number. This will make it more difficult for attackers to gain access to your devices or accounts, since the system will require not only a password, but also an additional PIN code.

See how many sites have information about you. Even though sites like MySpace have gone out of style, profiles created over a decade ago are still visible and accessible. This applies to any site on which you may have been active previously. If possible, remove outdated and unused profiles.

Doxxers can use phishing attacks to obtain home addresses, social security numbers, or even passwords. Be wary of receiving messages asking for personal information that appear to be from a bank or credit card company. Financial institutions never request such information via email.

WHOIS is a database of all registered domain names on the Internet. This public registry can be used to identify the person or organization who owns the domain, their physical address, and other contact information.

If you plan to operate a website anonymously without revealing your identity, make sure your personal information is kept private and hidden from the WHOIS database. Domain registrars may control privacy settings, so you should check with your domain registrar to find out how to do this.

If personal information appears in Google search results, you can request that it be removed from the search engine. Google implements this as a simple process using an online form. Many data brokers post such information online, usually for background or criminal background checks.

You can remove your personal information from data broker sites. Deleting data yourself without material costs can be labor-intensive. If you're pressed for time, start with the three major brokers: Epsilon, Oracle and Acxiom.

These databases should be checked regularly as information may be republished even after it has been deleted. You can also pay services such as DeleteMe, PrivacyDuck or Reputation Defender to delete your data.

Online quizzes may seem harmless, but they are often a source of personal information that users provide without thinking about the consequences. Some quiz questions may even be test questions for your passwords. Many quizzes ask permission to view your social media profile or email address before showing results. They can link the survey results to your real personality without caring too much about who is running the quiz or why it's best to avoid storing this data together. Mobile applications are also sources of personal data.

Many apps ask for data or device permissions that don't concern those apps at all. For example, it doesn't make sense for an image editing app to ask for permission to access contacts. Reasonable if it requests access to the camera or photos. But if an app requires access to contacts, location data, and social media profiles, be careful.

If possible, avoid publicly disclosing certain information, such as your Social Security number, home address, driver's license number, or any bank account information or credit card numbers. Hackers can intercept emails, so don't include your personal information in them.

The best defense is to make it difficult for attackers to obtain your personal information. You can test how easily you can be doxxed by finding out what information can be obtained about you. Find yourself on Google. Perform a reverse image search. Review your social media profiles, including your privacy settings. Check if any of your email accounts were involved in a major data breach using com.

Check your resume and personal websites to see what personal information is included in your professional profiles. If there are PDFs of your resume available online, be sure to exclude information such as your home address, personal email address, and cell phone number (or replace them with publicly available versions of such information).

Set up Google alerts for your full name, phone number, home address, or other sensitive information so you know if it suddenly pops up online. This could mean that you are a victim of doxxing. Be careful with information published on the Internet. Never post personal information on forums, message boards or social networks. It is naive to assume that the Internet gives people the freedom to say or write whatever they want.

People believe that anonymity allows them to express any opinions, no matter how controversial, without being traceable. But, as we have seen, this is not the case, so it is important to be careful when expressing your opinions on the Internet.

The most common reaction to doxxing is fear or even outright panic. There is a very clear feeling of vulnerability. Doxxing is specifically designed to make the victim feel threatened, panicked, and enraged. If you are a victim of doxxing, you can take the following steps:

Report the attack to the administration of the platform on which your personal information was posted. Please search the platform's terms of use or community guidelines for information on how to report this type of attack and follow those instructions. Once you fill out the form, save it for future use (so you don't have to repeat it). This is the first step to stopping the spread of your personal information.

If a doxxer threatens you personally, contact your local police department. Any data containing your home address or financial information should be given the highest priority for review, especially if there is credible evidence of threats.

Take screenshots or download pages that contain your personal information. Try to make sure dates and web addresses are visible. This evidence is important to you and may be useful to law enforcement and other interested authorities. If doxxers have published your bank account or credit card number, report it to the appropriate financial institutions immediately. The credit card issuer will likely cancel your card and send you a new one. You will also need to change your online banking and credit card account passwords.

Change passwords, use a password manager where possible, enable multi-factor authentication, tighten privacy settings for each account you use.

Doxxing can be emotionally draining. Ask someone you trust to help you figure out the problem so you don't have to deal with it alone.

Doxxing is a serious problem that has arisen due to the easy availability of personal information on the Internet. Staying safe in the online world isn't always easy. Using advanced cybersecurity techniques helps.

CYBERNETIC BULLYING

This is digital intimidation and bullying. It can take place on social networks, messaging apps, gaming platforms and mobile phones. These are repeated episodes designed to frighten, anger or shame those being persecuted. This: spreading false information or posting indecent photographs of someone on social media; sending abusive messages or threats via messaging platforms; impersonating another person and sending obscene messages on his behalf.

Cyberbullying leaves a digital trail - a record that can be useful and provide the evidence needed to stop the bullying.

Sometimes the other person may say that he was “just joking” or that you shouldn’t take his words seriously. However, if you are offended by his words or it seems to you that he is laughing not with you, but at you, then, most likely, such a joke has crossed the boundaries of what is permitted.

When bullying occurs online, it can result in unwanted attention from a wide range of people, including strangers. Wherever such behavior occurs, if it displeases you, you do not need to tolerate or ignore such a situation.

When a person is being bullied online, they feel as if they are being followed everywhere, even when they are at home. He gets the impression that he has nowhere to hide from his offenders. Such actions can have long-term consequences: psychological - the person becomes sad, feels awkward, seems stupid to himself or gets angry; emotional - a person begins to be ashamed of his hobbies or loses interest in them; physiological - fatigue (sleep problems) or symptoms such as stomach pain and headaches. Fear of ridicule or harassment from others may prevent victims from speaking up about the problem or trying to solve it. In extreme cases, cyberbullying can drive a person to suicide.

Cyberbullying affects many aspects of life. But all these problems can be overcome, and self-confidence will be restored.

If bullying occurs on social networks, you can block the harasser and send a complaint to the social network administrators. Companies that own social networks have a responsibility to ensure the safety of their users. It is useful to collect evidence - correspondence and screenshots of posts on social networks in order to confirm what is happening. In order to stop cyberbullying, it must be identified, and the most important step is filing a complaint. This will also show the harasser that their behavior is unacceptable.

If you are in danger you should contact the police. Think before you post anything online - this information can remain on the Internet forever, and then someone can use it to harm you. Don't give out personal details like your address, phone number, or the school you go to.

Review the privacy settings on your favorite social networks. You can control who is allowed to view your profile, send you private messages, or leave comments on your posts by changing your account privacy settings. You can report offensive comments, messages and photos and ask for them to be removed.

In addition to “unfriending,” you can completely block certain users so that they cannot see your profile or contact you. You can also choose a setting that will make certain users' comments appear only for them, without blocking them completely. You can delete messages on your profile or hide them from specific users.

On most of your favorite social networks, users don't receive notifications that someone has blocked them, restricted their access to your account, or reported them. People who are victims of any form of violence, including bullying, intimidation and cyberbullying, have the right to justice and to have the perpetrator held accountable.

In countries with specific cyberbullying laws, online behavior intended to cause serious emotional distress is considered a criminal act. In some of these countries, victims of cyberbullying may seek protection, a ban on the harasser's communication with them, or a temporary or permanent restriction on the harasser's use of electronic devices used to carry out cyberbullying.

TROLLING ON THE INTERNET

The term “Internet troll” generally refers to an online commentator or debater whose goal is to provoke conflict between others by posting controversial and outrageous comments. And although trolls have existed for a long time, they attracted the attention of most people with the popularity of social networks. Soon they appeared on various famous platforms.

In addition to ignoring outrageous troll messages, you need to know how to identify them. It is worth understanding that trolls are not those people who have an opinion opposite to yours or with which you disagree.

It's quite easy to encounter trolls because they are everywhere - on social networks, on online gaming sites, in the comment sections of news pages and in online forums. Online trolls come in many varieties, from people who post deliberately annoying or controversial comments to stir up controversy for their own amusement, to cybercriminals who pursue other malicious goals online.

Today, a well-known example of Internet trolling is the use of the topic of the COVID-19 pandemic by online criminals to spread controversial publications. In particular, trolls oppose vaccinations by sharing fake home remedies or even questioning the competence of medical professionals. It is worth noting that cybercriminals also use Internet trolling, for example, posting controversial content. However, their comments are usually accompanied by links disguised as the source of information, containing malicious software.

Internet trolling may seem innocent at first, but often the situation can worsen and escalate into cyberbullying or cyberstalking. Part of this may be due to the “online disinhibition effect,” where people talk and act online in ways they would never do in real life. In such cases, people feel little to no remorse for their actions because they do not see the impact on others and experience no real consequences for such actions.

“Don't feed the trolls” is a basic rule to follow when dealing with these criminals online. Otherwise, you may only make matters worse by giving trolls what they want: attention. While you might want to take part in the discussion, be prepared for your arguments to fall on deaf ears, because the goal of such people is not discussion, but reaction - mostly angry or anxious.

However, there are methods to protect your self from online trolls. Social networks Facebook, Twitter and Instagram offer tools to report trolls who deliberately bully other users, publish other people's personal information for everyone to see, use “hate speech” or violate other generally accepted principles.

Sites do not condone this type of behavior, so depending on the severity of the violation, moderators can impose penalties ranging from warnings and temporary bans to blocking the accounts of repeat offenders.

If internet trolling is happening on other forums, your first step should be to contact the service administrators, who have tools to deal with abusers. News sites have clear policies against offensive behavior, which trolls often violate, resulting in them being temporarily or permanently banned.

If Internet trolling turns into cyberstalking, cyberbullying, intimate harassment, harassment, or other behavior that may be contrary to various laws, you may contact law enforcement.

Internet trolling can often be a relatively harmless activity that some people engage in to gain the attention of others for the purpose of entertainment. In such cases, be aware of special tools designed to punish online trolls. In any case, criminals will think twice before doing this again, since Internet anonymity does not cover everything, and sooner or later everything will become known.

DIGITAL FOOTPRINTS

Every network user leaves traces of their actions and presence, even if they are lawful. These traces are called digital. Crimes committed using computer and network computer technologies are showing incredible growth, which is a great threat to ordinary citizens. Forensic capabilities are developing in proportion to the development of the IT sphere, therefore in forensic theory there is a tendency to study the subject of digital traces of criminal activity in the following main directions: - In in a narrow direction - this is the prevention, detection and investigation of crimes in the field of computer information: unauthorized access to computer information, creation, use and distribution of malicious computer programs, which in most cases are predicates for committing (or concealing) other crimes (theft, distribution of extremist materials , falsification of voting results, etc.).

In a broad direction, this is combating the commission of crimes using IT technologies. These crimes include: incitement to suicide using the Internet or inducement to suicide; remote theft in finance; calls for terrorist, extremist activities, mass riots; trafficking in drugs and weapons, pornographic materials; organization of gambling; crimes against the sexual integrity of minors, phishing, identity theft, information blockade, espionage and blackmail.

Digital traces in forensic science should be considered much more broadly. They are relevant when conducting procedural checks and investigating any crimes, regardless of the object and method of the offense, the category or form of guilt, the person's awareness or ignorance of their abandonment, as well as affiliation with one or another participant in the criminal process (suspect, victim or witness). Of interest are digital methods of proving criminal activity, the use of high-tech forensic equipment and specialized programs to obtain forensically significant information when examining sludge.

Unusual methods of proving such crimes, the objective side of which is expressed in the dissemination of any information or in public calls for illegal activities, also acquire specificity. This includes: inspections of users' social networks, their electronic devices and screenshots of pages that display all user data activity (correspondence, sent and received images, videos, documents, left "likes" and comments). Courts and juries perceive this practice positively because it is reliable and reliable.

A digital footprint should be understood as a set of unique actions that are performed in the information environment, including information left as a result of interaction with various network and telecommunication resources. A digital trace can be left by both an individual and a legal entity. Also, a digital trace can be defined as any forensically significant computer information. This is information (messages, data) that is in electronic digital form, recorded on a tangible medium using electromagnetic interactions, or transmitted through communication channels via electromagnetic signals.

Personal data remains in the digital space forever, and it is almost impossible to get rid of it, while leaving it is not the slightest difficulty. The statement “The Internet remembers everything” is proof of this. Digital traces are:

- video recording (both by the criminals themselves and produced against their will) of the preparation, commission, and concealment of crimes;
- billing information about connections between subscribers (subscriber devices);
- information contained in the memory (cloud storage) of a smartphone, phone of a participant in criminal proceedings;
- forensically significant information located in computer memory;
- metadata and digital information of various gadgets, allowing you to determine the location of the gadget and its owner; social networks as a source of forensically significant information;
- user browser history data;
- remote sensing of the Earth's surface.

A more specific expression of electronic digital traces are operating system and application software files, system registry files, logs, configuration files, settings, text documents, tables, databases, photo, audio and video files, program logs, cookies and other files contained in the system and components of the computer system unit itself.

The features of electronic traces include the fact that they: are one of the objective forms of the existence of computer information; always mediated through an artificially created object of the material world - an electronic information carrier, outside of which they physically cannot exist; many individuals can have remote access to them at the same time; copied onto various types of electronic storage media; are discovered, copied (duplicated), examined and used for the purposes of criminal proceedings only with the help of special scientific and technical means - means of searching, collecting, storing, processing, transmitting and providing computer information.

A digital trace does not have a spatial form, it has features of its internal structure and methods of transformation, and it is not available for direct perception. The extraction of digital traces, as well as their consolidation, analysis and research as forensically significant information for an investigation, requires persons with special knowledge in this area to provide consultation, assistance in seizure, forensic examination or interrogation as an expert.

One of the key benefits of digital crime traces is that they provide an objective and easily accessible record of a criminal's activities. This is especially important in cases where evidence is difficult to obtain through traditional methods, such as in cases of cyber crime. In these cases, digital crime traces can provide valuable information about the offender's identity, location and activities, as well as the time and date of the crime.

Another important aspect of digital crime traces is that they can be used to create a timeline of events related to a crime. This can be especially useful in complex cases where there is a large amount of information to process and many potential suspects. By analyzing digital traces, investigators can better understand the order of events and those involved.

Digital traces of crime are not always reliable. For example, a criminal may try to cover his tracks by deleting his Internet history, using a different device to commit a crime, changing his IP address, erasing metadata, and these are just the simplest methods of all.

Digital traces can be tampered with or altered, making them less reliable as evidence. This highlights the need for their proper seizure, storage, analysis and processing to ensure reliability, convenience and compliance with criminal law when used as evidence in criminal investigations.

The concept of digital crime traces is constantly evolving as technology advances, and it is imperative for forensic scientists to stay up to date with the latest developments in order to effectively use digital traces as evidence. Understanding the advantages and disadvantages of digital traces, as well as the legal and technical aspects of using digital evidence, is critical for forensic scientists and law enforcement agencies to effectively use digital traces as evidence in criminal investigations.

It is important to understand the ethical implications of using digital traces as evidence. For example, the use of digital traces may raise privacy concerns as individuals may not be aware that their activities are being tracked or recorded. There are privacy laws and regulations that govern the collection, storage, and use of digital traces, and it is critical for law enforcement agencies to be aware of these laws to ensure that the evidence they collect is admissible in court.

The use of digital traces may result in the collection of irrelevant or unnecessary information, which may place additional burdens on law enforcement and increase the risk of wrongful convictions. To address these issues, it is important for law enforcement agencies to have clear policies and procedures for the collection, storage, processing and use of digital traces, which include some principles regarding what types of digital traces are appropriate to collect, how they should be collected and analyzed, and how long they should be retained. By taking these steps, law enforcement agencies can ensure that they are using digital crime traces in an ethical and responsible manner, while providing valuable information to assist criminal investigations.

In the future, the use of digital crime traces is likely to become even more common and important as technology continues to evolve and become more integrated into our daily lives. This means that digital traces of crime will become an increasingly important aspect of criminal investigations, and forensic scientists must be prepared to use them effectively as evidence. Therefore, by understanding and accepting the advantages and disadvantages of this phenomenon, forensic scientists can effectively use digital traces as evidence in criminal investigations and stay abreast of the latest developments in technology and crime.

To effectively use digital crime traces as evidence, it is important that forensic scientists and law enforcement agencies work together. Forensic scientists can provide the necessary knowledge and experience about the nature and use of digital traces in criminal investigations, while law enforcement agencies can provide the necessary resources to collect, store, analyze and process digital traces. It is important to recognize that digital crime traces are not a replacement for traditional forms of evidence. Rather, they are an additional tool that can provide valuable information and assist in investigations.

The most effective way of investigation is a combination of traditional and digital evidence to obtain a complete picture of the crime and build a convincing evidence base. “Virtual traces” and methods of working with them will complement forensic technology, and the criminal law will undergo the necessary changes that will provide a mechanism for performing the entire range of actions with virtual traces.

SECURITY OF BUSINESS MODELS

The digital economy is shifting to platforms and digital ecosystems. The diversity of digital ecosystems is already large and most known ecosystems span multiple industries and includ different industry sectors, partners, competitors, customers and businesses. This also challenges traditional industry thinking.

The management and centralization approach is breaking down and unite mentality is emerging.

A digital ecosystem is a network of interconnected digital technologies, platforms and services that interact with each other to create value for businesses and consumers. It consists of various elements such as software, hardware, data and people that work together to facilitate digital transactions, communication and collaboration at various stages of the customer journey. These customer journeys can be interconnected, and the ecosystem can support a variety of activities, including e-commerce, social media, software solutions, hardware offerings, and digital entertainment. In a business context, a digital ecosystem can also refer to the set of digital platforms and technologies that a company uses to interact with its customers, partners and other stakeholders.

The digital ecosystem focuses on creating added value for customers by optimizing the data and workflows of various internal departments, tools, systems, as well as customers, suppliers and external partners. It must remove barriers to the customer journey and enable each participant in the ecosystem to use the latest technologies and systems to meet their individual needs.

The main goal of ecosystems is to offer customers a single, easy-to-use system that provides value through a variety of services, products and knowledge. This also allows platforms to grow exponentially and outpace the general market with multiple mechanisms involved.

This also means that different business models are possible as the ecosystem scales. From direct sales of products and services to advertising, subscriptions and much more. By better understanding the customer and redesigning the product offering, the number of services and products offered can be increased based on the amount of information received from customers. This makes digital ecosystems so powerful and also so profitable that the list of the most valuable companies in the world is led by companies that leverage the power of digital ecosystems. Here you will find Apple, Google, Facebook, Microsoft and many other companies that use their customer base and ecosystem approach to grow revenue and offer better products and services to their customers.

Since 2000, Amazon has continually built its digital ecosystem. First, the retail giant needed to build a gigantic server infrastructure around the world to be able to serve customers on its e-commerce platform. But Amazon soon began leasing server capacity to other businesses. This move led to the birth of Amazon Web Services (AWS) and was a major milestone for the company in creating this huge ecosystem that they now have.

Amazon used its own AWS infrastructure not only to provide infrastructure services to other companies, but also as a launch pad for all other services such as Amazon Prime Videos, Prime Music, Studio. This led to the rapid creation of services in the Amazon universe, as well as blocking many users. The advantages of these services were that they were the main users and received packages faster, had access to amazon music and could even watch series and movies from the main library.

Amazon later brought in many third-party companies to participate in the ecosystem. Just like with e-commerce, Amazon was the first to open up and allow even competitors to use this infrastructure of services and tools offered by the company. This brought them great success.

Successful digital ecosystems are value-driven. Sometimes these ecosystems didn't even have a monetization model at the beginning because they were customer-centric and understood before they even started pricing services or offerings. Characterized by a focus not only on customer service and personalized advertising of the company's offers. This means holistic operations and collaboration between departments and between services to integrate the customer journey as best as possible.

One of the main benefits of using a digital ecosystem is the ability to collect additional information about processes, customers and transactions. This makes data one of the key drivers for every digital ecosystem. The more you can learn about a customer, the better you can offer services, software, technology and tools to improve the customer's experience.

With the enormous insight that digital ecosystems gain from customers, suppliers and third parties, it is also possible to make that insight actionable. Automation is one of the key elements of reducing costs, increasing customer satisfaction, and offering new services to increase value flow.

Digital ecosystems exist to scale, and by limiting them primarily to countries or regions, you will never benefit from the platform and ecosystem. This means that digital ecosystems must also be built to enable collaboration across countries, regions and even languages. Sometimes even cultural barriers need to be addressed.

Due to the scale of digital ecosystems, it should also be noted that the mentality must be very dynamic. Ecosystems must quickly adapt and respond quickly to changing market dynamics otherwise the user base will move forward and switch platforms. Business intelligence, rapid decision making, and the use of new technologies and business models must be at the center of every decision. Before you start imagining yourself as an ecosystem builder, you need to take a deep dive into your company and your offerings. This also means that you need to determine which ecosystems are important to you and what role you will play in the ecosystem.

There are three different roles your company can play in the ecosystem. Ecosystem organizers take on the risk, complexity, and challenges of building a digital ecosystem. These are companies like Amazon, Alibaba and Ping that allow others to participate in the ecosystem and sell goods and services through the system.

Modular manufacturers contribute to the ecosystem and monetize value across different ecosystems. One of the most famous module manufacturers may be PayPal. Through their services, they offer various platforms and service ecosystems to have a single payment gateway so that customers can pay easily. A module manufacturer can add core services to ecosystems that meet the needs of consumers, businesses, and buyers and sellers in a specific sense.

The customer can be a person or business that benefits from the ecosystem. By booking Airbnb, you become a customer of the ecosystem that Airbnb has created and orchestrated.

Sometimes boundaries are fluid. So, for example, a Facebook user is both a creator (content) and a consumer (advertising). In addition, companies may sometimes use, sometimes orchestrate, and sometimes add services to multiple digital ecosystems.

There are three types of digital ecosystems. A functional digital ecosystem is typically built around a company's existing product or offering. A limited number of companies and partners (perhaps 10-100) participate in it. It focuses on the internal aspect. Due to its simplicity and ease of integration, it is the most widely used ecosystem. But this also has its limitations, since data collection and further integration are difficult, since in most cases it is a closed ecosystem.

Examples of such functional ecosystems can be found in the automotive industry, where platforms connect to digital services of partners, creating a product-centric smart and connected car ecosystem with a limited number of products. More advanced ecosystems are digital platform ecosystems. They can include millions of partners and also include many digital offerings.

These digital ecosystems are based on a data-first approach, allowing customer information to be used to further improve sales or develop new offerings based on the data collected. But the biggest difference is the common platform on which all partners participate and create their value. The ecosystem organizer offers a common platform on which all connected parties work together.

Google provides a common platform where developers, manufacturers and engineers can work together to create home appliances that use the Google Home platform to become connected and smart. Google itself develops tools such as the home speaker, but partners can also use the platform's ecosystem to offer their products and services.

Super platform ecosystems typically include many different industries, many different services, and try to connect the entire user journey with the ecosystem as best as possible. Most super platform ecosystems are owned by Apple, Google, Amazon and Tencent. WeChat showcases Chinese super app.

The application covers all important aspects of the user's life. It offers thousands of services and features within a single platform, including everyday banking, social networking, shopping, communication and more. With each new offer, WeChat becomes more integrated into everyday life, allowing for better data collection that can lead to new offers and bans.

CHALLENGES AND RISKS OF DIGITAL ECOSYSTEMS

While digital ecosystems have enormous potential for value creation and growth, they also bring with them a unique set of challenges and risks due to their size and complexity.

One of the main issues is privacy and data security. Given the enormous amount of data that is tracked, transmitted and processed within the ecosystem, there is a significant risk of data leakage, misuse and cyber attacks wanting to get their hands on this data. In addition, dependence on one or a few platform providers can lead to monopoly control, which in the long term limits competition and innovation, and existing movements also try to prevent this through regulation. There is also a risk for providers in the ecosystem (modular manufacturers) to become too dependent on the ecosystem for their business, leaving them vulnerable if the ecosystem fails or changes significantly. Similar problems for communities and companies were demonstrated by the examples of Twitter and Reddit.

For an ecosystem organizer, a serious problem and risk is the compatibility of various technologies and systems within the ecosystem. Inappropriate or inconsistent technology standards can have a strong impact, which is why Google and Facebook set their own technology standards and develop them independently. Depending on the business model, regulatory requirements are also an issue. Because digital ecosystems are complex and global, regulations regarding data protection, compliance, antitrust, and other relevant policies must be constantly monitored and followed. Countries are often not allowed to access various services.

Creating an ecosystem requires a broad customer base, consistent value creation, clear alignment between different partners, customers and technologies, and a highly flexible mindset.

Working on the Internet involves the use of countless passwords and separate logins, and regular requests for the same information when creating digital service accounts. There must be a safer and more effective way to protect against fraud. It is necessary to improve the method of digital identification and ensure its security in such a way as to achieve widespread use of this method. Given the range of digital identity initiatives underway today, past failures, and the privacy challenges that lie ahead, it is not surprising that outsiders are being cautious and cautious as well as inspired.

Banks in Sweden have successfully introduced a common digital ID card that is used by three quarters of the country's population. At the same time, some programs failed when faced with the unusual nuances of mastering new technologies and interacting with regulators and the public. There is a lack of consistency and coherence between different approaches. In this regard, it is difficult to make predictions about when a unified global digital identification system will appear, which will allow solving all problems of personal identification, or at least most of them.

Widespread adoption of digital devices with identification functionality would mean a significant improvement. Paper documents, without reliable authentication methods, are highly vulnerable to theft and fraud. Even standard security measures included in existing digital services often depend on basic authentication methods (such as weak passwords). When you consider that 87% of identity fraud in the UK today occurs through digital channels, it is clear that security practices must change as the digital economy takes hold.

Digital identity systems have the potential to be much more secure than the paper documents they replace because they rely on a secure cryptographic certificate approach. They may also be further protected by time limits and other customized restrictions to control access to certain services or types of personal data. Huge opportunities will arise if digital certificates are linked to the user's mobile phone, which becomes a universal and reliable source of digital identity. Additionally, these devices can be further secured with built-in biometric capabilities such as fingerprint or facial scanning. This will be an important milestone towards a sustainable, secure and accessible digital economy.

Creative approaches to using decentralized methods are being tested to avoid reliance on a large centralized database model and to more effectively manage and minimize these risks. Risks can be mitigated through architectural designs that minimize the amount of transactional data collected during identity verification. By establishing clear privacy principles up front and incorporating them into the design framework, the necessary protections can be built into these systems. This approach will also help increase end-user confidence in digital technologies and ensure their widespread adoption through the many benefits of digital transformation.

Trust in digital technology is as important as fundamental security controls. Technology companies can play an important role in building user trust, as many of these global brands are already trusted providers of authentication solutions on popular digital media. The challenges of implementing digital identity are not insurmountable.

ARTIFICIAL INTELLIGENCE AND DIGITAL IDENTITY OF FINANCIAL DATA

The trading process has evolved to a point where traders use complex parameters and combinations of factors to arrive at a decision. From social sentiment assessments, through technical indicators, to fundamental information, investing today is more complex than ever. Machine learning can make the entire process easier by analyzing large chunks of data, identifying significant patterns, and generating single insights that guide traders toward a specific decision based on predicted asset prices.

Financial markets tend to be unpredictable and even illogical. Due to these features, financial data must be considered to have a rather chaotic structure, which often makes it difficult to find stable patterns. To solve this problem, the algorithm must be equipped with as much objective information as possible. Modeling chaotic structures requires machine learning algorithms that can find hidden laws in a data structure and predict how they will affect it in the future. The most effective methodology to achieve this goal is deep learning.

Deep learning makes it easy to deal with complex structures and extract relationships that further improve the accuracy of the results. The digital economy is an established system of economic relations, which means that it is necessary to regulate many issues, especially those related to the openness of data and their protection. Work must be done in the areas of identification, authentication and digital identity management. For example, in the banking sector - providing remote access to bank services, including the introduction of unified approaches to verifying information provided by the bank when servicing clients, in electronic form.

As a result, we should predict an increase in the financial involvement of the population and an increase in the range of financial services. The competence of the digital economy at the state level should be the relationship between fast processes of introducing financial innovations (less than three months) and relatively slow procedures for changing the regulatory environment (at least a year), blurring the established boundaries of the financial market, increasing the complexity and fragmentation of the financial market structure. These problems create risks in the stability of the financial system.

Blockchain technologies are beginning to be used in the financial sector. Blockchain is one of the defining trends in the fintech industry. Distributed ledger technology was previously associated exclusively with cryptocurrencies.

Today, they are trying to implement blockchain in all areas where control over the transparency and security of transactions is necessary. Distributed ledger technology ensures the abolition of intermediation; increasing the speed of transactions; verification of transactions. One of the options for using blockchain in the credit market could be to determine the credit rating of an individual for approval or refusal of a loan.

Credit scoring is a popular tool for determining an individual's financial ability to repay the amount of debt over a certain period of time. The score is usually determined by credit union companies (a number of lending institutions), which typically analyze each type of financial transaction that an individual has made, whether that be a loan in general or a history of payment terms on the individual's various lines of credit. This general method is considered quite effective and is a common source of obtaining information about a person's creditworthiness level.

But there are certain factors that are neglected when calculating an individual's credit score in the classic way. For example, this is information about an individual’s current accounts in various banks. The credit scoring mechanism based on the blockchain framework has the potential to become more efficient. This mechanism, based on a blockchain framework, analyzes many aspects of an individual's credit and income history from the point of view of financial stability for efficient and accurate analysis. It will allow you to analyze not only the status of accounts, but also the inflows and outflows associated with them. Thus, it is considered that the loan amount is withdrawn from the bank for all purposes of the individual.

The bank directly interacts with the client when providing the necessary loan. In this case, customer data regarding information about several debit or credit cards, insurance, salary receipts are loaded by stakeholders into a blockchain framework created for a single individual. Data that has been uploaded to the blockchain is verified by all blockchain stakeholders as the source code is open source to verify the validity and accuracy of the data.

Stakeholders in this network are the primary respondents in uploading customer-specific transaction data into the blockchain network based on customer identification, which will then be used for cumulative opportunity identification or customer scoring. In the case when, in real time, a client approaches a bank branch with an application for a certain loan amount, the bank, based on the identification process, initiates a smart contract that receives transaction data from the blockchain based on a specific identification code, containing the client's complete transaction data.

The data is transferred to the agent. The agent in turn calculates several required information objects from the information fed to the machine learning model, which is a binary classification model that provides the probability of whether the customer will subsequently be able to repay the required amount or not in a certain amount of time. The predictions from the machine learning model are then taken into account by the bank to decide whether to approve the loan request or not.

The credit market actively uses financial technologies. For example, determining the credit rating of an individual for approval or refusal of a loan can become more efficient thanks to distributed registry technology.

DIGITAL SECURITY FOR ENERGY COMPANIES

Energy companies are a prime target for cyberattacks by states and cybercriminals seeking to exploit the sector for their political or economic gain. The energy industry has undergone rapid digitalization, providing new opportunities for cyber criminals. The attacks are fueled by the high value of energy industry data assets, as well as automated and poorly secured processes and networks. Key vulnerabilities in the energy industry:

- outdated software; lack of secure remote access;

- lack of regular monitoring of configurations and software;
- lack of differentiation of access rights;
- lack of solutions to control application launches;
- lack of means of recording information security events.

Objectives of information security in the energy sector:

- protection of technological areas for generating electricity and delivering it to end users;
- ensuring the security of corporate resources (information infrastructure, web resources);
- end device protection; protection of sensitive information and personal data;
- compliance with regulatory requirements;
- preventing information leaks; identifying internal abuses and disloyal employees.

Understanding which attack vectors most frequently impact an industry is the first step in building an effective defense system. The energy sector is notoriously slow to update infrastructure and software, making it a prime target for DDoS attacks and exploits.

Regular updates of operating systems and the use of various information security tools to proactively protect against network compromise. Continuous risk monitoring through a cyber threat intelligence source can help organizations gain additional insight into the nature of potential attacks, the actors involved, and which industries or companies are being targeted.

Effective cybersecurity training is another important measure to keep organizations safe. It is important to train employees to identify phishing and social engineering threats to ensure the security of information and accounts, thereby reducing the risk of hacking.

By staying aware of the latest security threats, installing up-to-date information security controls, maintaining visibility into their and third-party IT infrastructure, and maintaining proactive security and a strong culture of risk awareness, organizations in the energy industry can prevent potential attacks on their assets.

Cybersecurity solutions for the energy sector:

regular training to increase staff awareness of information security issues;

information security audit and network scanning tools to detect and prevent exploitation of vulnerabilities, timely patching;

correct network segmentation for better control of network traffic and increased efficiency of cyber security systems; protection systems to maintain process continuity;

Network Traffic Analysis to detect traffic anomalies and detect cyber attacks at early stages;

firewalls and intrusion detection and prevention systems (IDS/IPS) for protecting the network perimeter, blocking unauthorized access and detection of potentially malicious traffic;

WAF (Web Application Firewall) to protect web resources using application firewalls from attacks such as cross-site request forgery (CSRF), cross-site scripting (XSS), SQL injection and other threats;

endpoint protection to reduce the risk of infection by programs and viruses, encrypt information, and ensure compliance with policies;

organizing secure remote access to the network and creating an encrypted communication channel using cryptographic means of protecting regulatory information;

DLP systems to prevent leakage of confidential materials, namely analysis and blocking of data transmitted via email, instant messengers, Internet resources and other sources;

access management systems (IDM, PIM) to control the life cycle of accounts and differentiate access rights to network segments;

Network access control (NAC) solutions for device inventory, visibility and control of connections to the corporate network;

data classification systems to improve the security of sensitive information by classifying, identifying users who interacted with documents, simplifying access, searching and tracking data, and eliminating duplications;

using interactive traps to effectively detect APT attacks; SIEM systems for centralized monitoring of information security, collection and analysis of data from cyber security tools.

IOT ECOSYSTEM SECURITY

Providers of IoT services and devices violate the principle of end-to-end information security, which is recommended for all products and services. According to this principle, information security should be established at the initial design stage of a product or service and maintained until the end of its life cycle.

There are issues both on the device owner side and issues that developers need to think about. So, at the very beginning of operation, the user must replace the default factory password with his personal one, since factory passwords are the same on all devices and are not strong.

Unfortunately, not everyone does this. Since not all devices have built-in security, owners should also consider installing external security designed for home use to ensure that Internet devices do not become open gateways to the home network or direct tools for causing damage.

There is no secure IoT ecosystem today. Internet things are especially dangerous in the context of the spread of targeted attacks. Once attackers show interest, gadgets turn into traitors, opening access to the world of their owners.

Weaknesses of IoT:

- transition to electronic currency;
- power supply for sensors;
- standardization of architecture and protocols, device certification;

- Information Security;
- standard accounts from the manufacturer, weak authentication;
- lack of support from the manufacturer to eliminate vulnerabilities;
- use of text protocols and unnecessary open ports;
- use of unprotected mobile technologies;
- use of unprotected cloud infrastructure;
- use of unsafe software.

SECURITY IN METAVERSES

Although the concept of the metaverse remains vague, its popularity is rapidly growing. In this regard, concerns arose about the safety of the new metaworld. Cyber attacks will find their way into the metaverse, highlighting the need to ensure the security of immersive worlds.

The case of a user who was subjected to digital harassment prompted Meta to introduce a system of “personal boundaries.” At the moment, there are no generally accepted laws and accompanying penalties in the metaverse.

Another issue of interest to security professionals is user privacy. There are a lot of hacks and falsifications of various game accounts, so it is fair to assume that the new universe with a huge number of entertainment services will face a similar problem.

One of the key elements that need to be protected is the digital identity of each user. After all, the profile will contain much more personal information than a Google or Facebook account. The Metaverse will embody all digital life, with bank account and other sensitive data, where protection against theft will be a critical factor.

Equally important will be the guarantee that users cannot fake someone else's identity. The identity verification mechanism is important. However, it is still unclear how spoofing can be prevented in the metaverse.

Spoofing is a type of fraud in which the criminal disguises an email address, display name, phone number, or website URL to convince the victim that they are interacting with a trusted source.

Augmented reality equipment and other tools in this new digital world are greatly increasing the amount of data tech companies can collect. For example, an attacker can even gain access to information such as heart rate, eye and finger movements. User biometric data is particularly sensitive information that, unlike a bank card number and account password, cannot be changed.

Without proper attention to data protection, the metaverse will become another space where users will be attacked for profit. Given how difficult it is to protect intellectual property in the physical world, it stands to reason that copyright protection will be even more difficult in the metaverse.

No matter how sophisticated the techniques for circumventing security measures, businesses need to stay one step ahead of cyber criminals. There are security issues unique to the metaverse and technologies such as blockchain, cryptocurrencies and NFTs.

Non-fungible token, translated from English. - “non-fungible token” is a way of mastering digital art in the form of music, images, animation. A significant risk of NFTs comes from the possible purchase of counterfeit non-fungible tokens. Attackers may impersonate well-known authors and sell fake certificates of ownership.

There is currently no security available to protect the metaverse from malware. The issue of developing a large number of safety standards is especially acute: this must be done as quickly as possible.

The immersive virtual world today exists without laws. Therefore, it is impossible to compile a list of recommendations for protecting identity in the digital world. We can only try to predict some problems.

The metaverse will establish new patterns of behavior the attacker will be more privileged and will seek to hack the system, not people. Issues related to user identification and authorization will become even more pressing. Unfortunately, despite the widespread adoption of passwordless technologies and MFA, this problem has still not been solved in the real world, and the concept of metaverses will make solving it even more difficult.

DIGITAL HARASSMENT

With the development of metaverses, reports began to appear online about harassment faced by users of virtual worlds. At the same time, digital harassment often leads to the same psychological damage as regular harassment, but is much less regulated by law.

At the end of 2021, Nina Jane Patel from Britain created her own avatar in the Horizon Venues metaverse. In the gaming space, her character was attacked by three other avatars, presumably male. The woman's avatar was stalked and attacked immediately after appearing in the Horizon Venues gaming space.

A gang of three male avatars approached the character Jane had created and began to aggressively grope him. They also made sexual comments towards the woman and took screenshots. To escape from her rapists, Nina Jane Patel had to go offline. A woman began to suffer from anxiety after being digitally harassed. The problem of women's safety in the virtual environment has arisen.

Harassment is a current and extremely dangerous form of sexual harassment and compulsion to commit it. By their legal nature, such actions are the grossest interference in the private life of a citizen. Harassment may include such actions as: periodic unpleasant jokes, inappropriate and aggressive flirting, persistent attention, as well as hints and intimidation of sexual overtones, including direct physical contact with the object of harassment. In real life, harassment is subject to legislative regulation, although such regulation is not enough.

The situation with digital harassment in a virtual environment is worse. So far, only companies providing access to the platform are investigating cases of digital harassment. Being in virtual reality is governed by a user agreement that people sign to access applications. Accordingly, copyright holder companies and developers have complete “carte blanche” to solve problems that arise in the virtual environment (including the issue of harassment).

Microsoft has removed social centers such as Campfire, News and Entertainment Commons on the AltspaceVR VR platform, which helped people meet and communicate digitally. The radical decision was made in connection with the increasing incidence of harassment in virtual reality.

Also, by default, the company has assigned a “security bubble” function to each user of the virtual universe. The option helps to create certain physical barriers between contacting users and does not allow the personal space of each of them to be violated.

Additionally, the company has strengthened control over the entry of new users into the platform. A Microsoft account is now required to use virtual universe services. The company decided to technically synchronize accounts with the Microsoft Family Safety application. The solution will allow you to control children's access to VR applications.

THE DANGERS OF VIRTUAL REALITY

Virtual reality technologies require a special headset. This is “stand-alone VR in a smartphone” (like 3DOF Oculus Go helmets complete with a 3DOF controller) or PC VR (development of the SteamVR/OpenVR platform with a “Vive Pro/Cosmos” helmet and “Valve Index”, “Windows Mixed Reality” glasses, compatible with SteamVR, or helmets and glasses for simulators and business training.It is worth considering the question of whether the headset is so safe for the user’s health.

Let's start with the philosophical harm of virtual reality - escapism. Escapism is called escape (escape) from difficulties and boredom of life into a fictional world. Almost all gamers and fans of the virtual world can be classified as escapists. Escapism is not considered a disease. Such famous people as writer Leo

Tolstoy and musician Syd Barrett were escapists. John Ronald Reuel Tolkien considered escapism a necessary component of creative personal development. His statement is confirmed by the fact that a lot of virtual reality regulars write books. In this regard, a new, separate genre has emerged.

There are 2 types of escapism - voluntary and forced escapism. The significant difference between voluntary escapism and forced one is that with voluntary escapism, a person himself chooses the lifestyle of a hermit, abandoning the "vanity of the world." As an example, we can draw a parallel with psychoanalyst Karen Horney's theory of recluse as a neurotic reaction to life.

With forced escapism, the gamer is sucked into virtual reality against his will. Parallel: drinking, smoking, drug addiction. The user is not aware of the fictionality of the world around him. At the moment of returning from VR, diseases that have arisen against the background of its abuse, such as depersonalization and maladjustment, do not allow one to come to terms with reality.

There is a loss of one's own personality and orientation in the real world, and everyday skills disappear. Having become accustomed to easily "hammering nails" in a game, a person cannot hammer a real nail. There is a substitution of reactions to events, a devaluation of social attitudes. Virtual reality leads to neurotic diseases and complete withdrawal in VR, which leads to mental illness.

Having gotten used to killing easily in the game, the user can easily become a killer in the real world. In this regard, games containing scenes of violence must be banned. But among VR users the percentage of violence is lower than in other categories of citizens. In the virtual world the player is lost. His opinion of himself is formed by the feedback of other players, which in turn is based on his performance of fictitious tasks.

Getting used to the fact that strength, health and youth can be easily obtained or replenished by successfully completing a number of tasks, and if unsuccessful, start playing (living) again, the gamer stops paying attention to the real state of his physical health.

To reduce the impact on physical health, for gamers “hung” for a long time in virtual reality, development is underway to invent “full immersion capsules” - with massage and training of physical functions. Until such capsules are included with a VR helmet or glasses, the player can forget about hygiene and also miss the development of a serious disease.

Virtual reality negatively affects many psychological processes occurring in the human body. The disadvantages of virtual reality include deterioration of long-term memory. It's not just VR use that affects memory impairment. This pattern is observed among all active Internet users.

For example, just a few years ago, in order to find out about something you had to visit the library, find the right book, find the necessary information in it and write it down. As a result, there is more knowledge, but it does not stay with us because it is acquired too easily. Virtual reality promotes the development of attention, but somewhat one-sidedly.

VR has the most detrimental effect on the user's thinking. There is a substitution of concepts and reactions to a fictitious event. For example, a person who has learned to jump with a parachute in virtual reality does not realize in the real world that his gaming skills will not help him in this matter.

Manufacturers of VR simulator helmets (Varjo, VR-2 Pro, StarVR) drew attention to this strong impact. For example, firefighters, when using VR simulators, demonstrated excellent results in the final testing in VR. However, in life, when faced with a real fire, they were lost.

VR simulators are one of the important areas of using virtual reality. Therefore, manufacturers are looking for a way out of this situation. Helmets are equipped with additional trackers, treadmills, exercise machines (for sensitivity, the severity of a fire extinguisher), and controllers. A solution to this problem has not yet been found, but enormous funding is being allocated to search for it and, probably, in the near future, it will be solved.

Another disadvantage of virtual reality is that the scripts for games are written by people. Ordinary hired screenwriters with their own complexes in their heads. Scenarios for virtual games can be used as propaganda, imposition of opinions or thoughts. They are carefully controlled game scripts undergo a lot of checks before going on sale.

Despite this, there are many complaints about this or that game. In games, the user often wanders knee-deep in blood and sees victims with serious injuries. Subsequently, in the event of a car accident or other type of incident, the natural human reaction would be to provide first aid. However, a gamer, seeing such a picture, will not attach great importance to it. The thought of helping the victims may not even arise in his head; instead, he will take out his smartphone and begin filming everything on video.

It is worth noting that this behavior applies to those users who “live in VR” and do not use it from time to time.

This behavior is a huge disadvantage of the influence of virtual reality. We have not yet come up with a way out of this situation. VR game developers warn against overusing them. The player needs to have critical thinking, be soberly aware of his actions, where you are, and avoid addiction. However, at the same time, manufacturers are constantly improving VR games so that people are fully involved in them.

Physical harm from virtual reality is disputed by reputable lawyers hired by the production companies or their advertising agents. Therefore, it is almost impossible to hold them accountable.

It has long been an established fact that VR causes motion sickness, dizziness and nausea - especially during its first use. The reason for this is the discrepancy in the load that our brain can perceive. The actions taking place in virtual reality contradict the physical state of the gamer at this moment. For example, according to the game, the user jumps into an abyss, the brain visually realizes this, but in reality the user stands still.

To avoid side effects from the use of virtual reality in VR helmets, the frame rate (screen refresh) and tracking are constantly being improved. Manufacturers also warn that at the first cases of nausea or dizziness, you need to urgently take a break or completely abandon further play.

While immersed in virtual reality, a gamer may experience astigmatism. The reason for this is that the user's eyes become accustomed to looking at one specific distance in VR (the screen is in the same place). When removing the VR helmet, the user, looking at real objects, discovers that they are at different distances, as a result of which the eyes have to strain.

No matter how the screens are improved, no matter how many pixels are put into the picture, the images of VR glasses and VR helmets flicker. This contributes to the development of epilepsy. It is worth noting that manufacturers are investing a huge amount of money aimed at improving the safety of using virtual reality devices, but the risk will always be present.

Don't overuse virtual reality. If you feel unwell or are taking medications, you should avoid spending the evening playing your favorite game. You can cause physical harm to yourself and your loved ones.

DANGERS OF IMMERSIVE ENVIRONMENTS

Immersive - creating the effect of presence, immersion. Due to these properties, immersive theater can be considered as a performance in which the audience acts in the performance along with the actors, and not just watches what is happening on stage. They become not consumers of the spectacle, but participants in the action.

This format gives the viewer equal rights and responsibilities that previously belonged only to the actor. These are stories about the boundaries of ethics. Experience can have more than just positive characteristics.

The basic danger arises from the difference between the experience of classical theater and immersive theater. And here's why - there is an unspoken, but intuitively accepted and shared convention by everyone. Erfin Hoffman describes it: The action staged in the theater represents a conventional, invented illusion, which everyone knows very well. Unlike ordinary life, nothing real or genuine can happen to the characters presented on stage. Immersive formats violate this. An outdated, unspoken concept creates an illusion of security.

The safe space already has some risks. On a horror quest, you successfully plunged into an atmosphere of horror, ran from a maniac who suddenly jumped out, tripped, cut the skin on your face, or simply hurt yourself. There is little pleasure. This is an example of a participant self-harming.

In classical theater such a danger does not exist. There is another side. There are known cases in horror quests when participants reflexively hit the actors. A more dangerous psychological fear is not synchronizing with other participants, falling out of the performance, or ruining part of it for others. In the case of classical theatre, this risk would not exist.

Some events involve a high level of frankness. Moreover, the frankness is not of the character, but of the performer. The participant receives the right, and in some cases the obligation, to express his opinion. And as is the case with any public expression of an opinion, with the right comes responsibility for the words. And this responsibility can overtake the participant in a variety of ways. People may well change their minds about this person. Perhaps this previously hidden, but publicly declared opinion will affect his reputation at work, in his family and among friends.

The audience trusts the actors and the director when they ask for an action. But we must understand that these actions are aimed at achieving some goal, not a goal known to us. Most likely, this goal is aesthetic, and the author’s task is to implement his plan. And there is a non-zero probability that, using tools from role-playing games and psychotherapy to involve the viewer in the performance, the authors are only thinking about the idea.

At the same time, the tools can be quite powerful, and without subsequent support in individual cases they can cause retraumatization of the participant. Also, we must not forget that one of the goals of any artistic manifestation can be shocking, and in this case the author is unlikely to be inclined to think about the comfort or safety of the participant.

In the Scandinavian practice of role-playing games (the Norgs have a very powerful school, subsidized at the state level, and in some cases used as a propaganda tool), there is such a term as “bleeding” - the flow, transfer of emotions and motivations from the character to the participant. On the one hand, isn’t this the goal of an immersive performance - the deepest possible immersion? On the other hand, this is a direct path to retraumatization or at least a spoiled mood.

Entering the theater, the viewer signs an unspoken convention of trust, entrusting his life to the director. You can see how it looked like in the example of “Cargo 300”, where the authors made exactly the same conditions as Zimbardo, only they turned the settings to hard - also for the sake of artistic intent.

How is the security issue being resolved now? Yes, practically nothing. You can leave performance quests by waving at the observer at the camera. But this does not cover the other risks listed above at all.

Theaters are introducing signed consent forms. But they do not protect the viewer. They protect authors from legal retaliation and actors from unwanted physical contact. And vice versa, they give the author the right to violate your security. At some events, in particular at "Cargo 300", the availability of psychological support is indicated if necessary after the performance.

Security in immersive theaters is not currently enforced. But we can start with normative methodology. Do not ask participants to do anything that the criminal code considers a violation. And don’t do this to the audience yourself. We need a bilateral convention. If they “shoot” loudly, write that there will be loud, frightening sounds. If you use a strobe, write that visiting the event may not be very useful for epileptics. If visual deprivation (artificial limitation of vision) is expected, warn about it.

We need transparency in the rules. The rules of participation and behavior must be known in full and in advance, so that the decision about whether to go to the performance or not can be made on their basis before. And not when they call you a mongrel and draw a phallus on your forehead. The participant’s personality should not suffer and be humiliated. A person should not find himself in a humiliating position. The question of ethics should stop the author and clearly show him the limit.

When you play yourself, you not only take on a reputational risk, but you also simplify the triggering of all psychological triggers that may coincide with your previous, sometimes traumatic experience. Even though a layman is not accustomed to separate his ego from his character, the presence of a role still acts as a buffer. And such a buffer is better than none, especially if the event space contains additional mechanisms that allow you to separate yourself from the character.

Huizinga J. in “Man Playing” introduces the term “Magic Circle”. This is a special space and time where the rules of the real world give way to the rules of the game. A person who finds himself in it may well refuse to perceive the reality that exists outside of this space. Many people are familiar with extremely deep immersion in computer games or an extreme degree of concentration on a game of board games like chess or Go, when the surrounding reality ceases to exist. Working with the Magic Circle involves demonstrating a very clear boundary - having crossed this threshold, you find yourself in a space where rules are different from those in real life. Now you are obliged to comply with them all the time while you are within these limits.

The magic circle consists of many factors, since everything that is inside this abstract circle: sounds, lighting and the behavior of the actors should help the participant understand that having crossed the line, he, like Homa Brutus, is inside a space that is not related to the outside world, and that's all inside this circle helps him focus on the illusion.

And the outside, real world, along with all the ghouls and ghouls summoned by the lady, must remain outside and not interfere with his participation in the performance. And another very important thing in the Magic Circle and its organization is an extremely clear demonstration that the event is over. That's it, finish, leaving the circle, you left your character inside and now you must consider what happened not through his eyes, but through your own.

There must be a right to help. The immersion may be too deep, so much so that it becomes uncomfortable. In this case, the participant can subsequently return and not drop out of the action entirely. An actor can also exercise the right to suspend the self-expression of a participant who has become so immersed that he goes beyond the rules. The rules should always clearly state the right to exit the event. This helps the participant not to feel like a hostage to the theater, obliged to follow everything that is done to him there.

None of the proposed solutions eliminates the danger. But there is a way to combat this too - use a liberation exercise on the first beat of the event. It may be important not to leave the participant alone with the experience, but to help him share both the experience and emotions among other participants. Firstly, it will help to appropriate the result of the event, and secondly, to smooth out feelings or an unpleasant part of the experience by sharing it with others. Do not throw a person out into the street, but help turn everything that he has acquired within the action into, if not positive, then into constructive experience.

Read the convention carefully. It can be expressed in the form of rules of participation, “informed consent”. Understand what you are signing up for and adjust your perception of the safety of the space you go to for new experiences. If there is no convention at all, this is not a very good sign. If you have read the convention and do not understand something, ask questions before starting.

But please accept with understanding if the authors refuse to reveal the entire artistic concept. The effect of expectation and surprise is an important tool for the theater; the author will not reveal all the intrigue to the viewer, depriving him of pleasure.

If you have read the convention and did not find permission to leave the performance at any time in the rules, discuss this before starting. You are not a hostage to the theater. Leaving an event does not mean disrupting it, especially if this is noted in the rules.

To disrupt an event is to act against the rules, deliberately breaking them. It's worth looking for a way in the convention that you can show the organizers that you no longer feel unsafe, but you don't want to disrupt the performance and might continue to attend if that danger subsides. If there is none, but you think it’s worth being on the safe side, discuss this with the authors.

If the authors rigidly refuse to ask for help, signal danger, or leave the event, this may well indicate that the artistic concept is more valuable to them than you. If you are offered to play yourself, then all the psychological triggers will hit you.

INDUSTRIAL INTERNET SECURITY

As part of the future Industry 4.0 project, manufacturing and IT are increasingly merging. This entails stricter security requirements. Typically, hackers find backdoors into the corporate network through the interface between the office IT network and the production network.

A 2017 study by Kaspersky Lab showed that almost every third cyberattack is aimed at industrial control systems and thus against manufacturing companies. The number of malware increases every year, and with it the associated damage to industrial systems.

The recent case of a cyberattack on an automated system (SIS) by the Triton malware proves that such a scenario is absolutely possible.

In conditions where functional safety-oriented automation systems become the target of hacker attacks, mutual integration of the functional and information security areas is required. To do this, you need to develop a general strategy for the future.

Industrial control systems are currently exposed to many threats, which include, in particular: infection by malware via the Internet and internal networks; introduction of malicious programs through removable storage media and other external hardware; social engineering, i.e. influencing people in order to induce them to take certain actions; human error and sabotage; penetration into the system using remote maintenance tools; use of control components communicating over the Internet using the IP protocol; technical failures and force majeure; hacking of smartphones located in a production environment, as well as extranet components and cloud solutions.

Functional safety is the reliable operation of safety-related systems (controls) and other means of reducing risk. If a critical error occurs, the control system transfers the equipment to a safe state.

The requirements for the performance of safety-related elements of control systems are set out in the EN ISO 13849 group B standard as well as in the IEC 61508/IEC 61511/IEC 62061 series. Depending on the degree of risk, the corresponding protective measures are divided into different levels: performance levels (PL) and safety integrity levels.

In turn, the task of cyber security is to protect against attacks aimed at limiting the availability, integrity and confidentiality of data. The task is achieved through preventive or active technical as well as organizational measures. Underestimating information security aspects when organizing functional safety can have direct consequences for production equipment.

It is also possible to have an indirect impact on the production process and thus on the final product. Examples include pharmaceutical products or safety components for the automotive industry. This is where changes could have significant negative consequences for consumers. Therefore, the IEC 61511-1 standard requires an assessment of IT risks in process industry security systems.

The user must carry out an IT risk assessment using the NA method in accordance with NAMUR recommendations and implement the measures determined in this way. The user can analyze the safety system of the automatic control system in accordance with the current state of technology and fulfill his obligations in terms of diligent compliance with the requirements.

For both functional and access security, a potential risk analysis is first performed as part of a risk assessment, or more accurately an IT threat assessment. There is a significant difference in approach.

As part of the risk assessment, designers must take into account rather static risks according to the Machinery Directive, for example mechanical or electrical sources of increased danger. In turn, an IT security expert operates in a constantly changing environment. Attackers, using ever new methods, are actively looking for weaknesses in security systems, considered in the field of functional safety as systematic failures.

Another important aspect is the human factor. In the field of machine safety, there is such a thing as “reasonably foreseeable abuse”, when, for example, personnel deliberately prevent the operation of safety devices. In the case of large-scale cyber attacks on industrial installations, we are most likely talking about targeted criminal intent.

OPERATING SYSTEM SECURITY FOR DIGITAL ECOSYSTEMS

The problem of protection against unauthorized actions when interacting with external networks can be successfully solved only on the basis of comprehensive protection of corporate information systems. Secure operating systems belong to the basic means of multi-level comprehensive protection. Most information security software are application programs.They require operating system support to run. The environment in which the operating system operates is called the trusted computing base. It includes a full set of elements that ensure information security: the operating system, programs, network equipment, physical security measures and even organizational procedures. The cornerstone of this pyramid is a secure operating system. Without it, the trusted computing base is built on sand.

Organizing effective and permanent protection of an operating system is impossible without a preliminary analysis of possible threats to its security. Security threats to an operating system depend significantly on the operating conditions of the system and on what information is stored and processed in the system. For example, if the operating system is used to organize electronic document management, the most dangerous threats are those associated with unauthorized access to files. If the operating system is used as an Internet service provider platform, attacks on network software are very dangerous.

Operating system security threats can be classified according to various aspects of their implementation. Classification of threats by attack purpose: unauthorized reading of information; unauthorized change of information; unauthorized destruction of information; complete or partial destruction of the operating system.

Classification of threats based on the impact on the operating system: the use of known (legal) channels for obtaining information, for example, the threat of unauthorized reading of a file to which user access is defined incorrectly and, according to the security policy, access should be prohibited; the use of hidden channels for obtaining information, for example, the threat of an attacker using undocumented capabilities of the operating system; creating new channels for obtaining information using software bookmarks.

Classification of threats by the type of security vulnerability used by the attacker: inadequate security policy, including errors by the system administrator; errors and undocumented capabilities of the operating system software, including so-called trapdoors - “service entrances” accidentally or intentionally built into the system that allow bypassing the security system; previously implemented software bookmark.

Classification of threats by the nature of their impact on the operating system: active influence - unauthorized actions of an attacker in the system; passive influence - unauthorized monitoring by an attacker of the processes occurring in the system. An operating system is called secure if it provides protection against the main classes of threats. A secure operating system must necessarily contain means for limiting user access to its resources, as well as means for authenticating the user starting to work with the operating system. In addition, a secure operating system must contain measures to counteract the accidental or intentional disablement of the operating system.

If an operating system provides protection not against all major classes of threats, but only against some, it is called partially protected. There are two main approaches to creating secure operating systems - fragmented and complex approaches. With a fragmented approach, protection is first organized from one threat, then from another, etc. An example of a fragmented approach is a situation where an unprotected operating system (for example, Windows 98) is taken as a basis, an anti-virus package, an encryption system, and a registration system are installed on it user actions.

With an integrated approach, protective functions are introduced into the operating system at the design stage of the operating system architecture and are its integral part. The individual elements of the security subsystem, created on the basis of an integrated approach, closely interact with each other when solving various problems related to the organization of information security, so conflicts between its individual components are practically impossible.

A security subsystem, created on the basis of an integrated approach, can be designed in such a way that in the event of fatal failures in the functioning of its key elements, it causes the crash of the operating system, which does not allow an attacker to disable the system's protective functions. With a fragmented approach, such organization of the protection subsystem is impossible.

The operating system security subsystem, created on the basis of an integrated approach, is designed so that its individual elements are replaceable. The corresponding software modules can be replaced by other modules.

No user can begin using the operating system without identifying himself and providing the system with authentication information confirming that the user is who he claims to be. Each system user has access only to those operating system objects to which he is granted access in accordance with the current security policy. The operating system records events that are potentially dangerous to maintain system security in a special log.

The security policy must be constantly maintained in an adequate state, that is, it must respond flexibly to changes in operating system operating conditions. Security policy is managed by system administrators using appropriate tools built into the operating system.

Information protection is unthinkable without the use of cryptographic security measures. Encryption is used when storing and transmitting user passwords and some other data critical to system security over communication channels. Operating systems do not operate in isolation, but as part of local and global computer networks. The operating systems of computers on the same network interact with each other to solve various problems, including those directly related to information security.

Each of the functions of the protection subsystem is solved by one or more software modules. Some functions are built directly into the operating system kernel. There must be a clearly defined interface between the various modules of the security subsystem, which is used when the modules interact to solve common problems. Operating system meeting the security standard must contain a security subsystem that performs all of the above functions. Typically, the security subsystem can be expanded with additional software modules.

People and businesses increasingly rely on digital interactions, prioritizing convenience over security and privacy. Respondents created an average of 15 new online accounts during the pandemic, which equates to billions of new accounts created worldwide. Some 44% reported that they do not plan to delete or deactivate these new accounts, which will result in a larger digital footprint in the coming years, significantly expanding the attack surface for cyber criminals.

A similar situation can be observed with Industrial IoT (IIoT): by placing sensors throughout the plant, a production subject creates sources of a huge flow of data that needs to be stored, processed in real time, monitored for condition and safety, and controlled access to this data.

Digital ecosystems are becoming more and more functional and make it possible to cover more business tasks or satisfy more and more user requests. The downside is that all these subsystems need to be protected. And the question is not that we need to implement more and more information security systems to protect data. It is necessary that the security tools being implemented are also capable of processing this volume of data in real time."

Such requirements are no longer made by the IT departments of companies, but by the manager, who today does not want to wait for two hours for raw data to be uploaded to Excel, but demands that it be displayed in real time on a dashboard on a mobile phone. This requirement alone raises several questions: how to process such a volume of data in the "here and now" mode? How to ensure the security of this database how to control integration layers, user access, including privileged users? How to connect the manager's mobile application with this database without intruders getting in? As a result, a large number of questions arise for information security services.

Ecosystems are growing not only among ordinary users or business customers they are also growing among attackers. There are forums on the darknet, cloud services for hackers - a distributed network infrastructure guesses passwords or cracks hashcodes, similar to how cryptocurrency is mined.

Once it becomes unprofitable to mine crypto, attackers use the same cloud infrastructure to mine passwords. For example, a user is confident that his password, consisting of eight numbers plus a sign, is quite complex, but a regular video card can crack it in four hours. If we talk about a distributed mining farm, then it will crack a fifteen-digit password within 24 hours, and these facts cannot be ignored. Users should be aware of the rate at which risks are increasing.

Let's say you had one virtual infrastructure - remote workplaces for which it was necessary to provide cybersecurity, and now you have a hundred such infrastructures that form a single meta-universe, which is one of the main channels of data leakage. Soon, companies will have representation in meta-universes, just as each company today has its own website.

These offices will accumulate user data and confidential information, which will also need to be protected. Soon, companies will have representation in meta-universes, just as each company today has its own website. These offices will accumulate user data and confidential information, which will also need to be protected.

The growth of protected ecosystems is accelerating, and the means to protect them require powerful, multidirectional, attracting a variety of expertise. The team should not only be able to install an antivirus, but also understand the realities in which the business lives, and in which areas it should be protected in the first place. For example, an online store may have a simple payment system that is integrated through authorization on a social network.

In each subsystem, hackers can launch a virus (through the cloud platform, among other things). A small business, not to mention an ordinary person, simply cannot keep track of all the risks, or they do not have the budget to protect themselves. The level of inaccessibility of a full-fledged cyber reliability service for most market players is becoming too high.

In these conditions, businesses are increasingly turning to companies providing outsourcing services.

Risks in the field of information security should be included in every investment project. The technological singularity is the theoretical point at which man will lose control of technological progress, which in turn will become irreversible. In simple terms, in the near future, technology may develop so much that humanity will simply no longer keep up with it and understand it.

One example of technological singularity is NFT, a popular system for transferring rights to use digital objects. The further we go, the more similar technologies will appear: people either do not understand them or are not interested in them. A condition arises for an uneven distribution of the future: someone already lives in the future, where there is a struggle to protect highly effective digital assets, and someone uses basic means at hand and does not distribute patch cords for the router on time. A simple scanner can scan a “naive” user’s network within a minute and detect holes in the security system. Fifteen seconds and the virus is with you forever.

That is why information security should be taken into account in the business plan of an IT project at the stage of its primary protection to the investor, before calculating the PNL (Profit and Loss Statement - profit and loss statement). The later a lack of information security services is discovered, the more expensive it is to implement them and protect an existing service.

Another problem is the low quality of communication between business and information security. Often, physical security specialists are closer to the business than information security specialists.

How should the owner behave correctly in terms of information security allocate sufficient funds for the construction and maintenance of the information security system; vest high-level powers with information security team specialists and facilitate their dialogue with decision makers (the so-called Executive Sponsors); recognize the priority of information security in all internal projects of the company.

As the amount of data grows, interesting scenarios arise in the operation of various systems, for example, in the operation of a company's data leakage protection (DLP) system. This system is capable of not only controlling access to data, but also creating shadow copies of documents that pass through the system, analyzing them: who accessed this or that document, copied, changed, and so on. As a result, the DLP system has a storage system that contains copies of the company's most "interesting" documents. Hundreds of thousands of counterparties create hundreds of thousands of documents per day, so this storage system itself becomes a Big Data object, which, in turn, also needs protection.

Working with Big Data as an object of protection, we ourselves create big data, but in the field of information security, and the means of working with this data must be appropriate - the speed of searching for information must be measured in milliseconds. We cannot allow a situation in which Big Data works with billions of records and at high speeds, and the IT unit creates storage in which the file system cannot contain more than ten thousand files.

When ensuring the security of Big Data, you need to use appropriate tools that can work with such a volume of information.

The rule also applies to machine learning: one of the vectors of a cybernetic attack is faking a visual recognition system. This is clearly illustrated by the case of how in 2019 the Tencent team showed that it could trick Tesla's Autopilot into crossing a median by adding small, harmless strips of tape to the road surface.

It is impossible to implement a system that, based on machine learning, recognizes a person's behavior pattern and thus makes a decision about who is at the console. The technology is based on a biometric identification system, including recognition by mouse movements, camera, fingerprint and so on. In response, attackers will create a system that is based on the same machine learning technology and learns to fake the behavioral model of another user so that the system recognizes the attacker as one of its own.

Sandboxes are virtual machine systems that, to a virus or to an attacker, look like part of a corporate system, for example, an accounting department with hundreds of real jobs. An attacker, falling into this trap, sees many IP addresses, subnets, machines, ports are open on them, applications are running, and stalls, studying this “infrastructure.”

This gives the information security specialist a temporary advantage to detect the attacker's actions. Creating sandboxes is becoming increasingly complex as more and more subsystems have to be simulated in order to appear believable to a hacker. We have to create a fictional metaverse for hackers to get lost in. This requires enormous power. The average company cannot afford these costs, and cloud security providers are the solution.

An important task of information security is to build a system of priorities for business to protect key segments of the company. Any business can be divided into blocks, the priority of which is higher than that of others. The cost of downtime is quite easy to calculate: how much does the company earn per year?

For example, a billion rubles, of which five hundred million are earned on the basis of one block, two hundred and fifty on the basis of another, and so on. What happens if you stop this or that block for a day? You need to divide the amount of income generated by the block by 365. This is how potential losses in the event of an information security incident are calculated, which are then ranked according to the degree of criticality and likelihood of implementation.

You can build a risk map in monetary terms for any company. Such a tool allows a manager to quickly make a decision about which risks he allows and which he cannot tolerate, and, based on this, purchase the required solution that eliminates the occurrence of costly incidents.

Internal audit helps optimize costs and increase efficiency. As a result, information security indirectly helps the business, even at the assessment stage. You can also build a map of technical compliance with legislation by country, industry and local regulations. Any piece of legislation can be expressed in a finite list of requirements.

SOFTWARE SECURITY

The main attention in the theory and practice of ensuring the security of information systems is focused on protection from malicious destruction, distortion, theft and use of software and database information. For this purpose, problem-oriented methods and means of protection against unauthorized access, against various types of viruses and bookmarks, and against information leakage through electromagnetic radiation channels have been developed and are actively being developed.

This implies the presence of persons interested in unauthorized access to information in systems for the purpose of its illegal use. To solve the problem, methods, tools and standards for protecting programs and data have been created and are being actively developed.

Dangerous situations leading to loss of system functionality, accidents and catastrophes are considered. In such situations, the external functional performance of systems may not be completely destroyed. However, it is impossible to fully fulfill the functions and requirements for information quality.

In the systems under consideration, the safety of their functioning is determined by the manifestations of destabilizing factors that cause damage:

- technical failures of equipment and distortions of information from environmental objects and systems;
- failures and physical destruction of elements and components of hardware of computing systems and telecommunications;
- defects and errors in complexes of information processing programs and in data;
- gaps and shortcomings in the means of detecting dangerous failures and promptly restoring the working state of systems, programs and data.

Catastrophic consequences and failures of operation with great damage are possible in the absence of hostile persons interested in such disruptions to the performance of systems and software. They have their own nature, features and characteristics. Therefore, they require independent study and adequate methods and means of ensuring safety. In some systems, failures affecting safety may be deliberate destruction or corruption of information in databases.

Careful specification and assessment of the security of systems, software and information is an important factor in ensuring their effective and appropriate use. This can be achieved by identifying, defining and providing suitable characteristics taking into account the use and functional objectives of software tools and systems.

It is advisable to distinguish two classes of systems and their characteristics. The first class consists of systems that have built-in software complexes with strict real-time regulations that automatically control external objects or processes. The response time to emergency situations of such systems is usually calculated in seconds or fractions of a second, and the processes of restoring functionality must be carried out automatically (on-board systems in aviation, in some weapons and transport).

Systems of the second class are used to manage processes and process information from the environment in which specialist operators actively participate (administrative, banking, military headquarters systems). Acceptable response times to dangerous failures in these systems can be minutes, and restoration operations can be entrusted to specialist security administrators.

The concepts and characteristics of system security are close to the concepts of reliability. The main difference is that reliability indicators take into account all occurrences of dangerous failures, while safety characteristics should record and take into account only those failures that led to such a large, catastrophic damage that it affected the safe operation of the system.

Statistically, there may be several times fewer such failures than those taken into account in the reliability values. However, methods, influencing factors and real values of software reliability can serve as guidelines when assessing the safety of critical systems.

Damage from defects and errors in programs and data can manifest itself in systematic failures. The accumulation of such failures over time can lead to consequences that impair the functional safety of systems and their applications. Thus, the concepts of reliability and safety of complex systems and software come closer. With more or less identical sources of threats and their manifestations, these concepts can be divided according to the magnitude of the consequences and damage in the event of emergency situations.

The more complex the systems and the higher the safety requirements for them the more uncertain the functions and characteristics of their safety and quality. Uncertainties begin with customers, who, when formulating technical specifications and specifications, do not fully formalize and fundamentally cannot provide the content of absolutely the entire set of functions, characteristics and their safety values that should be present when the project is completed and the final product is presented to the customer.

These requirements are iteratively formed, detailed and clarified by agreement between all project participants due to the limitations of the primary source data and their changes under the influence of various processes at successive stages of the life cycle.

Changes and differences in personnel using the system and software further increase the uncertainty of safety values and the difficulty of predicting it, taking into account the many subjective factors of the various specialists involved in operation.

In the process of design, development and life cycle of the main functional tasks of the environment, these components develop and adapt over time, which is reflected in the need for adequate changes in methods, tasks and means of ensuring their safety.

An objective increase in the complexity of functions implemented by programs in modern systems directly leads to an increase in their volume and complexity of creation. According to the increase in the complexity of programs, the relative and absolute number of defects and errors detected and remaining in them increases, which is reflected in a decrease in the safety of their operation. As the complexity of the problems solved by programs increases, the impact of errors increases, which can threaten accidents and disasters in systems that perform critical functions for managing large, expensive and especially important objects or processes.

Orderly, regulated architecture design, development and maintenance of complex software based on modern technologies makes it possible to prevent and eliminate the most dangerous system, algorithmic and software defects and errors at the early stages of the life cycle, as well as to use safe software and information components that have been repeatedly tested in other projects.

To ensure the safety of critical systems, effective methods and tools are needed to prevent and identify defects, as well as certify the safety of using programs and databases, promptly protecting their correct functioning in the event of any defects and emergency situations.

The functionality of software tools can be ensured using the initial data that was used during their development, debugging and testing. Actual source data may have values that differ from those provided for in the technical specifications and from those used in the operation of programs and databases.

With such initial data, the operation of the PS is difficult to predict in advance, and various anomalies that end in failure are very likely ending in failures that affect safety. It is necessary to take into account the fundamental difficulties of analytical assessment and prediction of software safety values, due to the unpredictability of the position, manifestation and consequences of defects and errors in programs and data. This leads to the impossibility of reliable a priori analytical calculations of the security of software packages at high values.

The problem of achieving the security of systems containing real-time software is solved by using modern regulated technological processes and tools to ensure their life cycle. The structure, sequence and content of technological processes of life cycles in the standards are somewhat different, but the nomenclature of the basic components is almost the same, which allows them to be selected and applied taking into account the security of specific software projects.

To combat threats to the safety of software, it is necessary to study the factors affecting functional safety from defects and errors that exist and are potentially possible in specific systems and software complexes. This will make it possible to purposefully develop methods and means of ensuring the safety of critical software for various purposes while reducing the level of design and development defects in a realistically achievable manner.

The problem is solved through the use of modern methods, tools and standards that support analysis, design technology, development and maintenance of systems, their software and databases.

The complexity of programs and databases, as well as the available resources for their implementation, become indirect criteria or factors influencing the choice of development methods, the achieved quality and safety of software.

All stages of software development and maintenance should be supported by methods and means of verification and systematic, automated testing of program components. Testing is the main method of eliminating defects, measuring and determining the real characteristics of programs at any stage of their life cycle. The presence of sufficiently complete standards based on the totality of specification requirements and their step-by-step decomposition is a necessary basis for testing and measuring the safety and quality of software packages.

The development of systems and software must be completed by comprehensive testing and certification of the safety and reliability of systems with software, providing for the possibility of improving their characteristics through appropriate program adjustments.

Improving security is advisable by implementing procedures for analyzing identified defects and promptly restoring the computing process, programs and data (restart) after detecting anomalies and failures in the functioning of the PS. This can be facilitated by the accumulation, monitoring and storage of data on identified defects, failures and failures during program execution and data processing.

BASIC CONCEPTS AND FACTORS DETERMINING SOFTWARE SECURITY

Software tools must have economic, technical, scientific or social effectiveness of application, which in projects must reflect the main purpose of their life cycle in the system. This system efficiency can be described quantitatively or qualitatively, in the form of a set of useful characteristics of software, their differences from those available in other software packages, as well as factors and sources of efficiency. As a result, the purpose of use and the set of requirements of the customer and user when creating or purchasing software, as well as its intended purpose and scope of application, should be formalized.

In standards, effectiveness reflects the functional suitability of software. This characteristic is related to what functions and tasks the program solves to satisfy the user, while other design characteristics (including safety) are mainly related to how and under what conditions specified functions can be performed with the required quality.

During the system analysis process in preparing the technical specifications, the values of various factors, quality and safety characteristics should be selected taking into account their impact on functional suitability.

Improving the quality characteristics, including safety, requires some expenditure of resources (labor intensity, finances, time), which should be reflected in the quality characteristics - suitability.

The goals, purpose and functions of protecting a set of programs from failures are closely related to the suitability features of each type of software. In the process of system analysis and design, potential intentional threats to the operation of the software must be identified and the security level of this set of programs must be established. In accordance with this level, the customer and developers must select and install the required and necessary sets of methods and means for ensuring the security of the software, taking into account the limited resources for their implementation.

As a result, the formed requirements must provide equally strong protection against various real threats and the implementation of the necessary control measures and confirmation of the required characteristics of the suitability of a set of programs in the face of threats to the safety of the functioning of software.

To ensure the effectiveness of the system, it is advisable to base a set of security programs on the following general principles: protection of system hardware, functional programs and data should be focused on all types of threats, taking into account their danger to the consumer; the cost (labor intensity) of creating and operating a protection system should be less than the amount of the most probable or possible (on average) damage unacceptable to consumers of the system - the risk from any potential threats; a set of protection programs must have targeted, individual countermeasure components designed to ensure the safe operation of each individual component and task of the system, taking into account their vulnerability and the degree of impact on the security of the system as a whole; the system of protection programs should not lead to tangible difficulties, interference and a decrease in the efficiency of application and solution of basic, functional tasks by users of the system as a whole.

Characteristics of the environment, application areas of application of software packages, goals and objectives, level of automation of their functions and many other factors determine methods for ensuring the security of computer systems. The distinction between types of security is not always clear-cut and should be considered and taken into account depending on the specific functions of the systems, the security objectives and results, and the categories and characteristics of the situations.

Damage in failure situations is determined by vulnerability and violation of the correct execution of the purpose and required functions with limited resources for their implementation.

Countermeasures are limited to additional means of protection against failures, changing the ratio of requirements to various characteristics and redistributing available resources for their implementation.

The functions of systems and their software are implemented in an environment whose characteristics significantly affect the functional suitability of the programs. To perform the required functions of a software package, adequate initial information is required from environmental objects, the content of which must fully ensure the implementation of the functions declared in the system requirements. Since it is fundamentally impossible to create and use complex software systems without defects and errors, attention should be focused on the characteristics of defects in functional programs that determine the main purpose of the system.

The software security environment includes policies and programs for organizing the security of enterprises and systems, experience, special skills and knowledge that determine the use of the system. The environment also includes possible security threats that are known or suspected to be present in the environment. When formalizing the security environment, the following should be taken into account: the purpose of the system, including the functions of the product and its intended use; programs and data of functional tasks of the system, as well as components that are subject to system security requirements; the physical environment in that part that defines all aspects of the system related to safety, including measures related to protective equipment and personnel.

Based on the developed security policies, threat and risk assessments, initial data related to the security of the system environment and the main set of programs is generated: assumptions that the environment must satisfy in order for the system or software to be considered secure; security threats to assets, which would identify all environmental threats predicted on the basis of security analysis as related to the security object; threats, which are revealed through the concepts of the source of threats, the intended method of their implementation, preconditions for failures and identification of components that are objects of failures.

The following classification of failure situations is used: a situation that prevents the system from operating and functioning as required; a situation that results in a significant reduction in the performance, use and operation of the system or in the lack of the ability of personnel to cope with adverse operating conditions in which: severe situations or system overloads that can cause inaccurate or incomplete execution of tasks with great damage; a situation that leads to a decrease in the suitability of the system or to a reduction in the ability of personnel to cope with unfavorable operating conditions, the continuation of which may result, for example, in large distortion of information resources or reduction in functionality, overload or conditions causing a significant deterioration in the performance of the system or personnel; a situation that slightly reduces the safety of the operation and use of an object, but affects its reliability; a situation that has little or no impact on the functionality, performance, and capabilities of the facility or does not increase the workload of personnel.

The effort, resources, and time required to ensure consistency with customer performance requirements vary depending on the categories of failure situations. The degree of security of systems is characterized by the prevented and residual damage to the risk that is possible when destabilizing factors manifest themselves and specific threats to the safety of the system are realized.

This brings the concepts and characteristics of the degree of safety closer to the indicators of system reliability. The difference is that reliability indicators take into all failure occurrences, while safety characteristics should record only those catastrophic, critical or dangerous failures that resulted in a safety violation with great damage. In some cases, the consequences of failures may be useful to reflect the duration of the operational state of the system between failure events relative to the duration of use of the system, taking into account the time spent on detecting and eliminating failures (availability factor).

Destabilizing factors for system security are: failures and failures in computing equipment; viruses, glitches and failures distributed through telecommunication channels affecting information and functional security; changes in the composition and configuration of the system or substation equipment complex beyond the limits verified during testing or certification; system errors when setting problems for designing the suitability of the system when formulating requirements for the functions and characteristics of safety equipment; defects and errors in determining functions, conditions and environmental parameters; algorithmic errors in the design of security functions for hardware, software and databases when determining the structure and components of functional program complexes, as well as when using database information; errors and programming defects in program texts and data descriptions, as well as in the documentation for software components; insufficient effectiveness of the methods and means used to protect programs and data and ensure operational safety.

Complete elimination of the above threats to the safety of the operation of critical systems is fundamentally impossible. When creating complex software systems, the problem is to identify the factors on which they depend, and to create methods and means of reducing their impact on safety.

To ensure the security of systems, appropriate countermeasures are created - specialized systems and tools, which include a set of interrelated regulatory documents, organizational and technical measures and corresponding methods and software.

The available amount and distribution of resources for individual types of countermeasures have a significant impact on the overall security of the system achieved. When ensuring security, resources are used for the following purposes: control and correction of information defects; operational monitoring and detection of defects in program execution and data processing; placing and ensuring the functioning of the applied means of protection against all types of system security threats; generating test sets or storing tests to monitor the performance, safety and integrity of software during system operation; accumulation, storage and monitoring of data on identified incidents, attempts of unauthorized access to information, defects, failures and failures in the process of program execution and data processing that affect security; implementation of procedures for analyzing and monitoring identified defects and prompt restoration of the computing process, programs and data (restart) after detection of defects and system failures.

The customer is primarily interested in the functions, safety and quality of the finished final product - the system and software, and is usually not very concerned about how they are achieved. The required functional safety can be achieved in two ways: by using only final, final control and exclusion from delivery or by sending for rework products that do not meet the required safety and quality; through the application of regulated technologies and safety and quality systems in the design, development and manufacturing processes that prevent defects and ensure high safety and quality of products during their creation and/or modification.

The policy for ensuring and certifying the safety and quality of complex software should be based on inspections and testing of software life cycle technologies supported by regulated quality systems; functioning of the finished software product with a full set of documentation.

Functional suitability is the most critical, uncertain, objectively difficult to formalize and evaluate in projects characteristic of software packages, which significantly determines the requirements for ensuring the security of the system. The areas of application, nomenclature and functions of software complexes cover such diverse areas of human activity that it is impossible to completely identify and unify a fairly limited number of attributes for selecting and comparing the characteristics of software complexes with different purposes.

Functional suitability is a set and descriptions of attributes that determine the purpose, basic, necessary and sufficient functions of software, specified by the technical specifications and specifications of customer or potential user requirements. During the design process of a software package, suitability attributes must be specified in specifications. Attributes of quality characteristics can be the functional completeness of solving a given set of problems.

Functional suitability is determined by the quality of the relationship and consistency of the sequential formulations of the content and implementation of the main fragments in the chain of standardized requirements of the technical specification.

The functions of the software are implemented in the system environment. Its characteristics significantly influence functional suitability. To perform the required functions of the software package, adequate initial information from environmental objects is required. The requirement is to select the degree and strategy of test coverage of the structure and functions of software components, the set of execution routes and the entire set of programs for the subsequent verification and testing process, sufficient for the functioning of software with the required quality and accuracy of results under real resource limitations.

It is necessary to organize registration, accumulation of names, content of functions and execution routes of programs that have passed testing, as well as control of the proportion of untested programs.

The main task in software security design is to analyze and determine the necessary resources to create the software life cycle in accordance with the requirements of the contract and technical specifications.

A factor in the competitiveness of software is the relationship between the value (effectiveness) of an existing or proposed product from the perspective of its use by the consumer and its cost when created or purchased in a real market. To do this, it is necessary to determine the availability on the market of a range of software tools similar in purpose, to evaluate their economic efficiency, cost, applicability and safety, as well as the possible competitiveness of the proposed software product.

The safety of the software system is ensured by the creation of high-quality functional programs with a minimum number of defects and errors that affect safety. Security management of a complex project is carried out by managers. The project security manager ensures communication between the customer and specialists. His task is to determine and ensure complete customer satisfaction with regard to system security; The manager-architect of a set of security programs manages communications and relationships in the team, is the coordinator of the creation of components, develops and manages basic, functional specifications, maintains the project schedule and reports on its status, and initiates the adoption of decisions critical to the progress of the project.

Specifiers prepare descriptions of the functions of the corresponding components with a level of detail sufficient for programmers to develop program texts; developers of software components (programmers) create components that meet specifications and implement the required product functions; system integrators create the required large components or a set of programs as output.

Testers provide verification of functional specifications and perform phase and component testing of the project.

Managers ensure the synergy of components and the implementation of software versions. Documenters prepare and publish consolidated technological and operational documents in accordance with the requirements of the standards.

Technologists ensure the application of the quality system of a project or enterprise, monitor and inspect its use. Software must be put into operation and remain relevant until it is no longer needed. Their goals, conceptual framework and algorithms should not become outdated during development.

Preparation of program texts, their testing, integration, documentation and testing can be carried out mainly sequentially. This takes some time. In modern software projects, a greater or lesser proportion is made up of ready-made, proven components from other similar developments. This allows you to significantly speed up work and reduce costs for creating complex software packages.

DATA PROTECTION

Let's consider the main points of protecting information from unauthorized access. This is a work procedure in which only the user who has permission has access to information; we will call such a user legitimate; each legal user works only with his own information and does not have access to the information of another legal user; each legitimate user can perform only those operations that he is authorized to perform.

To organize such an order, it is necessary to ensure recognition of the legitimate user. This process is often called user authorizationю. User authorization includes three stages.

1. User identification.
2. User authentication.
3. Direct user authorization.

User identification is, on the one hand, assigning an identifier to the user - some unique attribute (or several); on the other hand, the process during which the user specifies the identifier assigned to him. Identification is the process by which a user identifies himself.

User authentication (from the English autentication - establishing authenticity) - establishing the authenticity of a user based on comparison with a reference identifier.

Authorized user (authorized person) - a user (person) who has received certain rights to work with information.

During the authorization process, the user's rights are determined for a legitimate user, that is, the data with which he is allowed to work is determined; operations that he is allowed to perform, etc.

User identification can be based on knowledge of some secret information (password, code); on the possession of some special item or device (magnetic card, electronic key); on biometric characteristics (fingerprints, retina, spectral composition of voice, etc.).

The knowledge systems of some secret information include software password protection mechanisms. Systems based on the possession of some special item or device (magnetic card, electronic key), as a rule, also require the user to know some secret information.

Systems based on the possession of some special item or device require the use of a magnetic card. The security system is equipped with a device for reading personal information (unique user code) recorded on a magnetic card.

The user's unique code is stored on a Proximity card equipped with a radio transmitter. A special reader constantly emits electromagnetic energy. When a card enters an electromagnetic field, the card sends its code to the reader, which the system then compares with the standard.

The most widely used protection systems are those using smart cards (SmartCard - smart card). The smart card's memory also stores reference information for user authentication, but unlike a traditional magnetic card, a smart card contains a microprocessor that allows some conversion of the user's unique code or some other actions.

In parallel with the development of smart card technologies, technologies based on the use of electronic keys are developing. The systems use the unique individual structural features of the human body to identify an individual. The systems include special reading devices that generate reference user identifiers, as well as devices or software that analyzes the presented sample and compares it with a stored reference.

A variety of devices have been developed that allow personal identification based on biometric characteristics. Fingerprint reading devices identify a person by the shape and number of details - the starting and ending points of lines on the finger.

Retinal scanners scan samples of the user's retina, focusing on unique blood vessels. Using infrared radiation with the brightness of a Christmas tree light, data is taken from 300 points in the retinal area of the eye, and the collected information is converted into a number. Voice verification devices build a mathematical model of a speaker's vocal range and use it to compare with a voice sample. Developers of such systems pay attention to solving the problem of deceiving such systems using tape recorders.

Hand geometry reading devices use light to build a three-dimensional image of a person's hand, checking characteristics such as the length and width of the fingers and the thickness of the hand. Biometric systems are difficult to implement and require storage of large databases, reliable image recognition technologies and expensive reading equipment. Therefore, such systems of protection against unauthorized access are used mainly in institutions that require special control of access to classified information.

User authentication is typically implemented using one of two schemes: simple PIN authentication or secure PIN authentication. Both schemes are based on establishing the user's authenticity by comparing the user's PIN code (PIN - Personal identification number) with a standard.

With simple PIN authentication, a PIN code is sent to a key (smart card). The key (smart card) compares it with the standard, which is stored in its (her) memory, and decides on further work.

The secure PIN authentication process is implemented according to the following scheme. The secure application sends a request to the key (smart card) for PIN authentication. The key (smart card) returns a random 64-bit number. The application adds this number modulo 2 with the PIN code entered by the owner of the key (smart card), encrypts it with the DES algorithm on a special authentication key and sends the result to the key (smart card). The key (smart card) performs the reverse conversion and compares the result with what is stored in its memory.

If there is a match, the authentication is considered successful and the user (application) can continue working. An electronic key is a physical device. It can be made either on the basis of a specialized chip, or on non-volatile electrically reprogrammable memory chips, or on the basis of microprocessors. Standards and technologies, in particular, technology for connecting devices based on the USB bus - Universal Serial Bus, allow you to have additional ports in convenient and easily accessible places on the computer and thereby contribute to the widespread use of hardware security devices.

Unique information is stored in the electronic key's memory. The software part of the security system detects the presence of an electronic key when starting the program and checks the correctness of the information contained in the key. The electronic key memory, in addition to unique information about the user (registration number, password, PIN code), may contain other parameters.

In order to counter the illegal distribution and use of software, security developers include information about the software in the electronic key, for example, the program serial number; version number; release (sale) date. If the program has the ability to work in demo mode, or in the mode of blocking some functions, the electronic key is supplemented with information about the number of times the application will be launched and the maximum time (date) of operation. Note that the electronic key can also serve to protect shareware software.

Technologies for remote reprogramming of the key's memory are used by developers, firstly, to counter the illegal use of programs. Remote reprogramming of the key memory allows the developer to maintain the software with the maximum degree of convenience for the end user. For example, along with a new version of a product, the user receives a special module that modifies the version number field in the electronic key’s memory.

The security module always compares the program version number with the corresponding field. This mechanism prevents illegal use of the program. The offender will not be able to use an illegally obtained copy of the new version of the product without reprogramming the memory of the electronic key.

It is also convenient for the user to transfer the software from working in demo mode to full functioning mode. After payment, the user also receives a special module that modifies the memory field of the electronic key responsible for such a transfer. In this case, the user is freed from the need to reinstall and reconfigure the application. Depending on the unique information about the user and special fields in the key’s memory, certain program functions are available to the user. Reprogramming the key's memory allows you to open or close access to certain functions.

Electronic keys also provide licensing in networks. A license is the right to use the program agreed upon when purchasing a software product. Network software developers strive to earn income from each copy of the program installed on a local network workstation. Users have the opportunity to install a licensed copy on the server and use it from any workstation. In these cases, developers receive inadequate profits from the sale of the software product.

This problem can be solved using special programs - license managers. Control of such programs rests with network administrators and is often not protected from fraud. Therefore, it is necessary that the product control is carried out by the developer himself.

To do this, you can store the license counter, as well as the maximum number of users of the licensed application, in the electronic key's memory in separate, write-protected fields. A system using such an electronic key allows you to control and limit the number of stations operating simultaneously with a protected program.

The reason hindering the use of software and hardware protection is the high cost of additional hardware devices. Usually these are expensive reading devices, so-called readers. Therefore, success in the market of hardware and software protection systems is ensured by those manufacturers whose electronic keys are more convenient and cheaper.

In practice, two methods of hacking software and hardware protection are mainly used: disabling (hacking) the software part of the protection; emulation of an electronic key. The first method of hacking is to remove (modify) from the protected application, in whole or in part, the codes associated with the protection mechanism. For example, sometimes it is enough to remove the commands for polling an electronic key and the commands for comparing with a standard from the program.

Electronic key emulation is a method of hacking by emulating the operation of an electronic key using software or hardware. An emulator is a program that performs functions usually implemented by some external device. The emulator program is implemented in such a way that it returns the "correct" responses to all calls to the electronic key to the protected application. The result is an electronic key implemented only at the software level.

To protect against electronic key emulation, it is recommended to use a chaotic order of information exchange between the protected application and the electronic key. Typically, the emulator interacts with a protected application either through the API entry point for calling the key, or by replacing the driver for working with the key.

HARDWARE SECURITY

The current concept of hardware-based security approaches relies on software built into the hardware, so hardware vendors and the research community need to change their mentality. The security of firmware should be treated the same as the reliability of software.

Computer systems include hardware and software: physical components that perform a fixed set of operations; logical elements consisting of data and instructions that define scenarios for performing hardware operations; as well as input data for them. Each individual function can be implemented using various combinations of hardware and software components, or entirely in hardware. The combination of hardware and software determines the properties of the function: system performance and security.

It was believed that it was hardware protection that best resisted potential attacks. This is reflected in long-standing hardware security modules (HSMs), such as the tamper-detecting and attack-resistant IBM CryptoCards, as well as Intel Software Guard Extensions (SGX) and ARM TrustZone.

The physical nature of the components means that once a device has been shipped to customers, it will be very difficult to correct potential defects, forcing hardware designers to act conservatively and thoughtfully. All this contributes to a feeling of additional security and greater confidence in protection compared to using software. Immutability is the ability of functional properties to resist change in their original architecture.

Since the physical implementation of hardware is a collection of electronic circuits and transistors, the hardware can be said to have inherent immutability: hardware-implemented functions cannot be changed by changing a few bits in memory. If an attacker wants to change the way the equipment functions, he must change it physically, which requires direct physical access to the victim. This state of affairs is reassuring, since making physical changes indicates obvious external interference.

Immutability is doubly beneficial because the hardware does not need to implement a Turing machine. Equipment has an inherent bias towards simplicity and economy. Because it involves physical implementation, having extended or unused functionality results in additional costs, creating an incentive to avoid excess capacity. Therefore, hardware logic most often implements functionality that is strictly sufficient to perform prescribed tasks without including arbitrary operations. All of this helps limit the potential damage caused if the hardware is compromised or malfunctions: the state of a hardware switch in a circuit can be changed from "off" to "on" by an attacker, but the switch cannot be reprogrammed in any completely different way.

Software, on the other hand, has a full-featured mechanism for doing something significantly different from its intended functionality. As a result, compromised or defective software gives the attacker access to a Turing-complete environment where randomly assigned functions can be performed.

Privileges refer to the ability to observe and control the operations of other components. This definition differs quite subtly from the characterization of privileges at the kernel capability level as opposed to user privileges, since software with higher privileges usually covers the operations of programs with lower privileges. Hardware and software privileges differ in that hardware and software cannot perform the same set of procedures.

Privileged software has the ability to control, start, stop, and interrupt non-privileged programs, as well as monitor (read, write) their execution status. Likewise, hardware that has a software execution engine has the same ability to manage and monitor the status of any programs it runs.

Modern computers have a universal, multi-layered architecture, starting with hardware and firmware, virtual machine hypervisor, operating system and ending with applications. The hypervisor is protected from the operating system kernel, which is protected from applications. The hardware in this stack occupies the most privileged position and is protected from vulnerabilities and attacks initiated at less privileged software levels.

There is a hybrid type of implementation of computing functions - firmware, or embedded software. The term “firmware” was proposed by Asher Opler in the 60s of the 20th century. Firmware has a number of common properties with software, since it is implemented in the form of software instructions that are executed on a Turing-complete general-purpose hardware processor.

To better understand hardware, firmware, and software, let's compare four dimensions of these components: immutability, privileges, efficiency, and cost.

Immutability characterizes the ability to change the functionality of a component. If with hardware immutability is its inherent property, then with firmware and software the situation is different. Immutability here is provided by some other component (hardware or software). For example, the firmware address space is typically closed to applications, and in many cases even to the operating system, either by a hardware control monitor or some combination of hardware and software control monitors.

Based on this, it can be argued that only the hardware is unchanged, while the firmware and software can be deliberately changed by certain components of the system or subject to changes due to design and implementation flaws. This eliminates the possibility of attacks during the delivery of the product even before it reaches the user. But even in this case, the hardware of the compromised device remains unchanged. Trojans introduced by the developer or manufacturer cannot be removed by firmware or software.

Privileges are determined in advance. They characterize the ability of a component with higher privileges to observe and control the execution of programs on an element with lower privileges. Since all software must run on hardware, it has higher privileges than firmware and software. Firmware resides on the hardware side of the hardware-software interface and has higher privileges than software, including the operating system kernel and applications. Thus, hardware privileges are the highest, firmware privileges are medium, and software privileges are the lowest.

Efficiency determines what productivity an implementation provides depending on the amount of certain resources, for example, electricity. Hardware implementations are more energy efficient than software implementations and provide higher performance with equal power consumption. Despite the fact that firmware and software are less efficient compared to hardware units. Firmware is closer to the hardware and can have access to special hardware features and facilities, making it more cost effective than software. For example, processor firmware (microcode) does not depend on context switches and the operating system scheduler, unlike conventional application software.

The hardware cost of each system is typically fixed, and the additional cost of deploying software is virtually zero. As a result, systems containing more specialized hardware are more expensive to manufacture, increasing their price to the end user. Faster systems using hardware accelerators are more expensive.

Firmware provides interoperability between many different computer system interfaces. Interoperability means that different component implementations will be able to communicate with each other normally because they all adhere to a standard interface. Implementing this interface using different combinations of hardware and software components allows manufacturers to create different products with different cost-effectiveness ratios.

For example, network cards perform the same function, but more expensive and faster products may contain different accelerators and offload technologies, making it easier to process packets faster. They consume less power, freeing up general-purpose compute cycles on the main processor. Specialized cryptographic accelerators have approximately the same properties. Operations that do not require high performance can be implemented in firmware. Since all these options do not affect the interface, they can be interchanged without changing the software or other hardware components.

Another important advantage of firmware is the ability to update or fix hardware errors to implement additional functions and eliminate defects. Much of the high-level functionality of a variety of consumer devices, from webcams to thermostats to home routers, is implemented at the firmware level, allowing for in-service updates to be installed to meet customer needs. For example, an important condition for choosing a particular smartphone model is the time during which the manufacturer undertakes to eliminate vulnerabilities found in the firmware by releasing appropriate updates.

The key to hardware safety is that it is not changed by software, which happens naturally.

Many functions of modern equipment are in practice implemented at the firmware level and are implemented iteratively: that is, first - SGX (Software Guard Extensions), then - SGX2. There is no longer any need to replace components because defects in the hardware can be corrected by changing the firmware. As a result, hardware has both the added benefits (flexibility and upgradeability) and the disadvantages (complexity and variability) of software.

Devices traditionally thought of as non-programmable (Turing-incomplete), when equipped with firmware (the introduction of a general-purpose processor), become Turing-complete, and if compromised, they can perform functions that were not intended at design.

One such example is the keyboard, which on an Apple device is turned into a keystroke recorder using simple software. When hardware functions are implemented using firmware, this affects the immutability of the hardware and weakens its resistance to attacks.

Computer peripherals such as disk drives, keyboards, mice and printers are generally considered too simple to be compromised and used for attacks. However, these devices increasingly offer functionality implemented by firmware, which leads to vulnerabilities.

Hard drives and solid state drives, which are usually thought of as simple block devices, contain a lot of embedded software. During an SSD security analysis, a Crucial MX100/MX200 device was subject to a successful firmware flash attack using several undocumented vendor-specific commands.

The discovered vulnerability allows a hacker to remotely and secretly intercept any data from a disk without leaving any traces on the computer. The hacker doesn't need physical access. Unlike ordinary malware, in this case the malicious code was contained in the firmware, so even a complete reinstallation of the operating system will not eliminate the infection. In 2013, it was demonstrated that hidden backdoors could be installed in a mechanical hard drive.

In 2006–2007, it was shown how it was possible to gain partial control over a Broadcom network adapter by modifying its firmware, and a little later the scope of this attack was expanded to gain complete control over a computer using a vulnerability in the Broadcom NetXtreme network adapter. The vulnerability was discovered in the firmware that processed the Alert Standard Format protocol, a little-known procedure designed for remote administration.

Video cards in the Video BIOS (VBIOS) component also contain firmware that is loaded and executed by the CPU in much the same way as a regular BIOS. Attempts have been made (an example is nvresolution) to configure VBIOS in such a way as to improve resolution through the video buffer driver. However, video cards can be used by hackers to execute malicious code, thereby avoiding traditional malware detection.

The GPU and video memory create a complete environment for executing malware, while the shared memory and CPU are used as additional resources for carrying out attacks. In 2013, researchers introduced into a computer a program to intercept keystrokes on the keyboard, which was executed not by the central processor, but by the graphics processor.

Various devices communicate with other components through buses such as PCI and USB. Devices connected to these buses provide common, albeit rather complex, functionality to automatically detect and configure them, as well as resolve conflicts between individual components. This functionality is usually implemented at the firmware level and becomes a source of various kinds of vulnerabilities. In 2006, for example, the special role of PCI expansion of read-only memory (ROM) was explored. VBIOS also falls into this category.

The corresponding part of the device firmware can be loaded by the operating system during the initialization process. It has been shown that due to a lack of firmware signature verification, a PCI card ROM extension can be re-flashed by malware. After this, the board can be used to carry out various pre-boot attacks, including manipulating the operating system kernel when connected to another computer.

The existence of a large number of different USB devices is explained by the fact that the USB interface offers advanced and flexible functionality. The USB interface allows you to emulate almost any type of component, unlike the SATA interface, which can only connect storage devices unless the operating system is compromised.

A group of researchers demonstrated the BadUSB concept, which involves reprogramming USB devices and then attacking the computer to which they are connected. The researchers were, in particular, able to reprogram one device to emulate another - for example, to emulate a keyboard, which began to direct a destructive input sequence to the victim's machine.

The vulnerabilities arise due to a lack of signature checking in the firmware of USB devices. Thus, malware hosted on one machine can use USB devices to infect others. It is able to change the firmware of a webcam or USB drive with subsequent infection of the next machine to which the corresponding devices will be connected. Lack of firmware integrity control is very widespread. Of the 52 families of chips and 33 actual devices, only one family implemented a primitive form of protection.

Compounding the problem, users tend to pay less attention to updating the security of their peripheral devices compared to traditional software systems - the main operating system and services. While most operating systems and applications offer automatic updates to protect systems from known vulnerabilities, firmware updates for peripheral devices such as hard drives or Bluetooth/Wi-Fi adapters are much less common and must be managed by users themselves. The main advice when undertaking such updates is that they should only be initiated when there is a clear need for it. Therefore, they are installed quite rarely.

When the AMT and ME vulnerabilities (CVE-2017-5689) were discovered in 2017, it caused great concern among security professionals as it was simultaneously revealed that both ME and related vulnerabilities may have been present in systems as early as 2008.

An integral part of Intel AMT is an application (trustlet) that runs in the ME environment and allows you to remotely control a computer. This extremely important functionality was implemented in firmware, which can be overwritten and modified in the way the hacker needs. As a result, the attacker gains remote control of the system regardless of what security software is present in the operating system.

Located at the hardware level of a compromised system, Intel ME enjoys unlimited privileges over all other parts of the system. In fact, you cannot be completely sure that malicious code has actually been removed. Security researchers have been actively studying Intel ME since 2009 and have coined the term “third ring rootkit,” which hides code embedded in ME with higher privileges than any other computer software or firmware.

The injection attack exploits a vulnerability in the memory recovery technology found in Intel processors. There is a possibility of incorrect memory reassignment, which should be prohibited. The memory recovery feature that facilitated the attack allows system software to reassign DRAM when it conflicts with the physical address range mapped to I/O devices. The original memory recovery technology did not take into account the need for proper access control and verification of the memory used by Intel ME.

While Intel addressed this vulnerability by encrypting ME memory and attempting to prevent further ME isolation compromises, other vulnerabilities in the ME firmware kernel (such as CVE-2017-5705, 6, 7) led to subsequent firmware compromises and facilitated the execution of arbitrary code. In 2017, Intel introduced new Innovation Engine (IE) technology in the Lewisburg chipset. Unlike ME, it only allows execution of Intel firmware. IE is targeted at OEMs, potentially increasing the number of chipset firmware vulnerabilities.

Chipsets, which are not simple non-programmable elements of the motherboard, implement complex functionality. They contain a number of mysterious firmwares that most users have very little idea about.

The firmware that is processed by the central processor, unlike other chips, will be called host firmware. Compared to chipset firmware, host firmware, known as BIOS/UEFI (Unified Extensible Firmware Interface), is more than just displaying the boot screen and initializing the computer hardware. Even after the system boots, a significant portion of the host firmware continues to run in SMM (system management mode), which runs highly privileged software that implements critical low-level system functions such as power management and hardware monitoring.

Because SMM code operates with privileges that exceed even those of the operating system, it is a target for attacks. On older motherboards (manufactured before 2006), the SMM code could be corrupted by malicious kernel code because the BIOS program could not hide the SMRAM (system management

RAM), where the SMM code runs, from normal/system software. In the SMRAM Control Register (SMRAMC), the D_OPEN bit determines the visibility of the SMRAM, and the D_LOCK bit locks the entire SMRAMC and D_OPEN register until the next reboot. On some motherboards the D_LOCK bit was not set.

Although all this was corrected in subsequent motherboards, the weaknesses in the SMM firmware did not end there. Since 2008, SMM exploits have been detected regularly. Later compromises were due to the failure to protect SMM from various unrelated mechanisms. For example, the memory recovery flaw used to compromise Intel ME was also used to attack SMM. Another compromise of SMM using a cache poisoning attack has been discovered.

Typically, system software can configure memory-type range registers (MTRR) to control which areas of memory are cached and which are not. However, for SMRAM no differences were made. Thus, an attacker has the opportunity to modify the SMM code copied into the cache without direct access to SMRAM. The next time the modified code is executed in SMM and performs the necessary manipulations on the current copy in SMRAM. To resolve this issue, a new register system control range register was created. It was only accessible from SMM and could configure SMRAM caching properties.

In 2009, researchers discovered that poorly written SMM code could call functions outside of SMRAM, leading to the potential for arbitrary code execution in SMM. To prevent this, a new control was added to the MSR_SMM_FEATURE_CONTROL register, the SMM_Code_Chk_En bit, so that the ability to run non-SMRAM code in the SMM could be configured in the original SMM code.

The peaceful period lasted until 2015, when another SMM vulnerability was discovered, this time related to the fact that SMM needed to accept external arguments. If the passed pointer is used without verification, the SMM code can be fraudulently written to the SMRAM designated by the pointer, making attacks easier.

All this combined forced Intel to offer a high-level solution in the same year - the SMM transfer monitor (STM). Instead of removing all vulnerabilities in SMM, STM aims to reduce privilege escalation opportunities through SMM by reducing the privileges of SMM code by monitoring it using a monitor.

After performing the necessary checks with the STM monitor, the SMM code behaves as expected. However, the usefulness of STM was not so convincing due to the fact that many different parties were involved in this process: those who wrote universal monitoring code that checks SMM code specific to different models (in the context of the existence of many different suppliers and models); those who determined how to coordinate between OS developers, BIOS developers, and hardware vendors, since STM checks can only be performed after all components are consistent. Numerous vulnerabilities discovered (complications related to firmware; motherboard technologies, such as secure boot via BIOS/UEFI; Intel Boot Guard technology implemented via Intel ME) do not allow us to consider the firmware reliable.

The processor has never been a purely hardware solution. Microcode, which can be thought of as another layer of hardware instructions, is increasingly being used to perform complex operations and implement new functions. It turns out that even if only vendor-verified updates are allowed, the hacker controlling the process can still choose to update in a way that makes it easier for him to carry out an attack. But, not a single one of the latest processors met the security criteria when carrying out attacks.

The danger of embedding programs into equipment can be analyzed from two sides: statics and dynamics. The first concerns the persistent storage of firmware, and the second concerns the security of the firmware execution environment during firmware execution. One of the key advantages of firmware is the ability to update it. However, embedded programs must run in volatile memory, and therefore need to be isolated from other programs. All this can be neglected if the firmware is considered part of the hardware.

As long as the firmware provides an update interface that is accessible to lower-privileged components, including the system operating system, there is a possibility of corruption. Although many of these interfaces only allow updates whose integrity has been verified using cryptographic means, there are various ways to bypass certificates, leading to compromise.

Since firmware itself is just a program, it inherits vulnerabilities that can be common to all types of programs. Memory corruption refers to a wide range of attacks where software defects can allow an attacker to modify a program's memory in a way not intended by the original developer. Own code and data can serve the hacker's purposes. This happens because the firmware must be loaded into volatile memory to be executed, even if it is stored in an immutable location. Memory safety is still an open question, not to mention less formalized firmware development. A typical example here is the latest ME vulnerabilities: multiple buffer overflows occur in the core ME firmware.

The firmware may not have physical isolation. There is only logical isolation from conventional software running on the same system, which leads to defects and vulnerabilities. This is in contrast to Turing-incomplete hardware, which does not share resources with software or is physically isolated.

Direct memory access (DMA) refers to the firmware of all high-bandwidth devices. To avoid the CPU becoming a performance bottleneck, the CPU memory controller allows devices and system software to configure the memory ranges that will be available to both the device's processor and the CPU. The device's processor can then move data autonomously.

The direct memory access provided by controllers creates a hole in already partitioned spaces - opening up memory to USB devices, SATA storage and network devices.

Embedding software into hardware is a concern in itself, but what makes the situation even worse is that the architecture and implementation of most firmware remains proprietary and largely undocumented. The security community relies primarily on reverse engineering to at least partially uncover details. This opacity hides potential problems from the public, while actual attacks are not necessarily carried out using available information.

The unknown does not contribute to strengthening security. Rather, it may result in serious vulnerabilities going undetected because security researchers must expend additional effort to obtain basic information before they can detect and disclose weaknesses.

Firmware attacks show that physical access to a system is not necessary to compromise a system: the desirable property of hardware that requires physical access to be modified no longer works. This is completely contrary to the generally accepted idea that hardware is immutable. Additionally, software security depends on the underlying hardware. Because the threat model of a computer system assumes that the hardware must be reliable, compromised hardware undermines all security guarantees. Thus, embedding programs into hardware leads to failures of both hardware and software.

Firmware attacks target persistent storage and are static, affecting immutability. If embedding programs into equipment did not exist, then there would be no update mechanisms - accordingly, attacks of this kind would be excluded. Other attacks target the firmware runtime protection system and fall under the category of dynamic attacks. Without embedding programs into the hardware, such attacks would fail because the hardware does not need a shared address space and is immune to memory violations. Consequently, this attack vector would also be eliminated.

The simplest way to ensure security is to avoid firmware. But there are many non-security reasons for using firmware. Firmware opens the door to a variety of implementations that strike a balance between efficiency and cost, which is critical to the survival of the computer industry. Having hardware that is partially upgradable in the field has many important benefits that cannot be ignored.

Hardware without upgradable firmware may contain errors. One of the Specter vulnerabilities cannot be eliminated by updating the firmware (microcode), since it is built directly into the hardware logic. Thus, the ability to patch hardware is a security benefit of firmware. The benefits of embedded software outweigh the security risks, and therefore, hardware with embedded software must seek methods to provide the same level of security as pure hardware implementations.

Since embedding software into hardware is inevitable, it is important to recognize that the vast amount of code that performs hardware functions deserves the same (or even more) attention as conventional software. Highly secure, low-level software components are often opaque in their functionality. Their proprietary nature prevents open auditing and security review.

Low-level privileges encourage implementation of functionality that is complex and unrelated to the original design. The concept of hardware-based security approaches relies on programs built into the hardware. Therefore, hardware vendors and the research community need to change their mentality: firmware should be treated the same as regular software.

Security design principles widely applied to software can be applied to firmware. Public oversight helps minimize issues arising from opacity. Some open source frameworks (such as coreboot and OpenWrt) act as reference points for secure firmware design.

When risks that cause harm are identified, reducing the damage they may cause is as important as preventing them. Firmware privileges can be managed at an even lower level for granular access control. To address the issue of insufficient separation, a least-privilege approach can be taken to further consider an improved firmware model that further abstracts away software and does not share functions with access control.

As with conventional software, the main reason for vulnerability is complexity. Traditionally, designers of equipment that was difficult to fix have adopted technological economies of necessity.

Before you trust a device, you must test its behavior against a predefined set of specifications. The functionality of an increasingly large part of modern equipment is implemented at the software level. This trend has a negative impact on the security of future computer systems.

SAFETY IN THE ENGINEERING ENVIRONMENT

The relevance of the study of the socio-anthropological foundations of technical safety is due to the need to ensure human safety in technical reality, since technical structures must function without a threat to the life and health of the subject of technical activity. The internal contradiction of technology safety consists in the unity of two aspects: the content of the first is the absence of threats to humans from technology the second aspect presupposes the absence of threats to technology from humans.

Within the first aspect, the main attention is paid to the technical and technological parameters of technical structures, the design, construction and operation of which should not harm a person and correspond to his biological, psychological and social characteristics.

The second aspect is related to the analysis of the causes of erroneous actions of the subject of technical activity. We are talking about clarifying the limits of trouble-free operation of equipment, the possibility of its compliance, adequacy with the structural characteristics of the subject, which acts as a link between these aspects. Therefore, the problem of technology safety in philosophy involves the study of the content of the human factor, the destructive influence of which is currently considered as a threat to the existence of not only technical, but also other components of social existence.

In the technogenic reality, people, when creating complex technical structures, often forget about the limitations of their social, psychological and physiological capabilities, embodied in the samples of technology they created and imposing certain boundaries to ensure their safety. Security cannot be unlimited; it always exists in a certain space of human parameters.

Solving the problem of rational interaction between man and technology encounters a number of difficulties. Even M. Heidegger warned that it is impossible to treat technology with indifference, as a tool, that technology has its own claims to man - to what he should be in order to best meet its requirements.

Anthropological restrictions form the human factor of technology safety, the effect of which can be destructive in the case of deformation of its individual components, or positive in the case of compliance with anthropological safety measures.

There are three groups of qualities, ignoring which is the basis for the occurrence of errors in the interaction between man and technology: physiological - the general physical condition of a person; psychological - personal characteristics of a person, with the characteristics of his psyche, psychological processes occurring in his nervous system; ergonomic - caused by inconsistency between the characteristics of a person and the machine part of a technical system.

A person in modern production is included in a production team with a complex structure determined by the nature of the equipment he serves. This determines the need, in the process of a comprehensive study of the "man - technology" system, for a detailed analysis of the functional structure of the work team in order to determine the degree of compliance with the nature of the technology used by it. Also important are the tasks of analyzing the functional responsibilities of each team member, developing practical methods and means of psychological training for workers to effectively perform functions associated with high psychophysiological and moral stress.

Particular attention is paid to the problems of psychological preparation of work teams for servicing complex equipment, the creation of criteria for assessing the psychological readiness of workers to effectively use technology, the study of issues of psychological compatibility of individual workers and the patterns of formation of cohesive work teams, as well as the conditions for effective team management.

ARTIFICIAL INTELLIGENCE AND CYBER SECURITY

Artificial intelligence (AI) involves information systems performing decision-making and learning tasks, similar to the intelligence of living beings

Neural network is an interconnected set of artificial neurons that perform simple logical operations and have the ability of machine learning

Machine learning (ML) is a technique for training an information system based on provided datasets without using predefined rules, and is a special case of artificial intelligence. The general task of machine learning is to build an algorithm (program) based on the provided input data and given correct/expected results - thus, the process of operation of the ML system is divided into initial training on the provided datasets and subsequent decision-making by the already trained system.

There are several methods of machine learning, for example:

Supervised learning is a method of machine learning that uses labeled data sets (classified objects with selected characteristic features), for which a certain “teacher” (a person or a training sample) indicates the correct question-answer pairs, on the basis of which it is necessary to build an algorithm for providing answers to further similar questions

Unsupervised learning is a method of machine learning in which labeled data sets are not used, the correct question-answer pairs are not specified, and the information system is required, based on the known properties of objects, to find various relationships between them

Semi-supervised learning is a method of machine learning that combines a small number of labeled data sets and a large number of unlabeled ones. This approach is justified by the fact that obtaining high-quality labeled data sets is a fairly resource-intensive and time-consuming process.

Reinforcement learning is a special case of supervised learning, in which the “teacher” is the operating environment that provides feedback to the information system depending on the decisions it makes.

At the same time, other algorithms can be used in machine learning, such as Bayesian networks, Markov chains, and gradient boosting.

Deep learning is a special case of machine learning that uses a complex multi-layer artificial neural network to emulate the functioning of the human brain and natural language processing, speech recognition and visual images (English computer vision). Computer vision is currently widely used in security systems, vehicle and passenger control. Natural language processing and speech recognition systems help voice assistants Siri or Alice answer user questions.

Big Data is a large amount of structured and unstructured data in digital form, characterized by volume, velocity of change and variety. To process Big Data, specialized software tools can be used, such as Apache Hadoop / Storm / Spark, Kaggle, NoSQL DBMS. It is believed that in order to increase business value when using Big Data, it is necessary to move from heterogeneous data to structured information, and then to knowledge (information).

A processed, structured and labeled dataset obtained from a relevant Big Data array is a necessary (and one of the most valuable) components for machine learning in modern systems.

Deep data analysis is structuring and extracting useful information from a heterogeneous and unstructured mass of data, including Big Data.

Fuzzy logic is the use of loose rules and fuzzy answers to solve problems in artificial intelligence systems and neural networks. Can be used to model human behavior, for example, to narrow or limit the search conditions for an answer to a question depending on the context.

Having examined the basic definitions and principles, let us move on to the issue of practical application of artificial intelligence systems in cyber security. The use of artificial intelligence in information security is justified by two factors: the need for a prompt response in the event of a cyber incident and the lack of qualified cyber defense specialists. If a company does not have a 24-hour shift of information security analysts on duty, then without a system for rapid autonomous response to cyber incidents it will be difficult to provide high-quality protection outside of working hours.

Before an attack, hackers can perform a diversionary maneuver - for example, launching a DDoS attack or active network scanning, distracting cybernetic specialists. In such situations, a cyber incident response system based on artificial intelligence will help which can simultaneously process a large number of events, automate the routine actions of analysts and provide a quick response to incidents without human intervention.

Thus, the IRP/SOAR Security Vision solution uses algorithms for predictive response to cyber incidents: a trained system allows you to predict the attack vector and its subsequent development in the infrastructure, show trends, and then automatically stop malicious actions and give advice to analysts.

Artificial intelligence-based security systems are indispensable for identifying anomalies by analyzing logs, data from SIEM systems or SOAR solutions. This information, with data from already processed and closed incidents, will represent a high-quality labeled dataset.

Classic anomaly analysis systems are built on some rules pre-set by operators: for example, the volume of specific traffic is exceeded, a certain number of unsuccessful authentication attempts, a certain number of consecutive positives. Detecting anomalies can help protect user data - for example, an online banking service can collect and analyze data about customer patterns (characteristics, patterns) in order to quickly identify compromised accounts.

Financial organizations can also use machine learning and artificial intelligence systems to conduct assessments (scoring) of borrowers, analyze financial risks, and in anti-fraud systems.

Another model for using artificial intelligence systems in cyber security is working with insiders. Knowing the typical behavior of the user, the system can send a warning to analysts in the event of a significant change in the employee's work pattern (visiting suspicious sites, being away from work for a long time, changing the social circle when corresponding in a corporate messenger).

Security systems equipped with computer vision and speech processing will be able to promptly notify security about attempts to pass through the checkpoint by strangers or employees using someone else's passes, analyze the work activity of employees using web cameras, and evaluate the correctness of communication between managers and clients over the phone.

Artificial intelligence-based systems are also used by cyber criminals. There are known fraudulent methods of using Deep fake (creating a realistic virtual image of a person) to deceive anti-fraud systems, faking voices for fraudulent calls to relatives of attacked persons with a request to transfer money, using telephone IVR technologies for phishing and theft of funds.

Elements of artificial intelligence are also used, which allow attackers to increase their privileges much faster, move through the corporate network, and then find and steal data of interest to them.

DIGITAL RESILIENCE

Digital sustainability means using technology in everyday business applications to protect the environment. People around the world are striving to reduce the environmental impact of digital technology and sustainable development. To achieve digital resilience, businesses are using advanced analytics. Businesses with digital sustainability goals can use digital processes, tools and forecasting models to weigh the potential benefits against the environmental impact of achieving them.

These businesses can strive to minimize the potential impact of their operations on the environment while still providing useful goods and services to consumers. Digital sustainability allows organizations to embrace environmentally friendly technologies without compromising their profitability.

As businesses move to the next generation of smart, data-driven digital technologies, there is a growing need to understand the entire lifecycle of products and applications in terms of their environmental and social impact. Consider the example of developing digital applications such as a file sharing application. Every time you run code for a file sharing application, carbon emissions will be generated. Basic storage and infrastructure will also contribute to the carbon footprint. The size of the file and the way it is transported between geographic regions and delivered across multiple hops and networks all contribute to the total.

The way information is presented across multiple devices, as well as hardware specifications and UX/design all contribute to the carbon aggregate. All of these factors require a rethinking of processes, products and services, and a more holistic approach to developing, delivering and managing sustainable digital solutions. For a designer, this will mean creating optimized code.

According to the fundamental view, this could mean modernizing the infrastructure, using a green cloud, or successfully leveraging the benefits of the cloud, such as using serverless engineering.

From a social perspective, this will mean building trustworthy and moral AI systems to schedule elements that improve serviceability, such as reducing document size while driving or web video in standard definition, rather than higher quality, finally managing the start of the process. complete the life cycle, be it simply declaring an informed choice or creating a robust biological system.

The way businesses operate is changing as a result of digital sustainability. Businesses are becoming increasingly environmentally conscious, recognizing the impact of digital operations on long-term environmental sustainability.

At the same time, businesses are beginning to recognize the importance of contributing to the environment, allowing them to develop digital sustainability plans that include both consumer and environmental goals.

The thoughts of customers must be closely monitored by the business. Customer preferences often influence how people spend their money. When customers value environmental protection, businesses strive to make sustainability a public priority. Appeal to consumer attitudes refers to an indicator of how a firm cares about the same issues as consumers.

A company's desire to impress customers may lead it to take a political stance or support a social agenda.

With digital resilience, companies can reflect customer desires without compromising their long-term performance. Adopting digital solutions that reduce a company's environmental footprint can improve its long-term prospects.

Consumer goods companies often rely on supply networks to develop and distribute their products to customers. Companies have always preferred to provide products to customers as quickly as possible, even if this speed comes at the expense of the environment.

Businesses can use technology to improve their supply chain without negatively impacting both local and non-local environmental conditions. Increased automation is often used in digital sustainability projects for supply chains.

Automated technologies can help improve process efficiency, as well as increase supply chain speed and virtually eliminate human error. Businesses that move their online databases to the cloud may also require fewer servers to achieve the same results, resulting in lower carbon emissions.

The same tactics that help firms develop a positive attitude towards the environment can also help them increase their customer base. As a result, companies that embrace digital sustainability practices can expand their impact.

Companies can also use digital sustainability systems to help remote staff in other ways. Whenever possible, many companies that have success managing remote teams choose virtual meetings over in-person meetings. Remote meetings reduce the need for transportation costs and reduce the environmental impact of physical transit.

Likewise, computerized workstations eliminate the need for paper, ink, paper clips, and other office supplies that are often thrown away after a single use. Digital resources have a direct beneficial effect on corporate operations: employees can work on the same online resources at the same time, data is shared instantly, and internal corporate communication is simplified.

Taking a careful look at your operations is critical to making digital resilience work for your company. Firms are investing heavily in remote monitoring and management software, which allows them to simultaneously improve company efficiency and environmental sustainability by consolidating IT support with managed service providers.

These organizations can support remote workforces while managing employee IT tasks through advanced IT automation, scripting, and patch management, eliminating the environmental impact of workplace energy consumption.

In a home or business context, smart electrical grids regulate and minimize overall energy consumption. Land use analysis technologies can help limit deforestation and avoid land misuse. Improved local weather forecasting leads to higher annual crop yields;

Smart recycling methods reduce waste in landfills and also increase the reuse of products. Contactless entry includes lighting and heating devices. Improved traffic management and parking structures can help minimize fossil fuel use as well as improve road safety.

SYSTEM SECURITY ANALYSIS

Systems analysis is an essential tool for identifying and mitigating security threats in the digital landscape. By taking a structured and methodical approach to threat analysis, security professionals are better equipped to identify potential vulnerabilities and develop effective strategies to mitigate them.

One of the key benefits of using a systems approach is that it allows analysts to take a holistic view of the security landscape, taking into account factors such as the organization's business goals, technology infrastructure and relevant regulatory requirements.

Using data-driven tools and techniques, such as machine learning algorithms and advanced analytics platforms, analysts can identify patterns and trends in threat activity that may not be obvious. This allows you to anticipate and respond to emerging threats before they can cause harm. By incorporating systematic analysis into their security programs, organizations can more effectively manage risk and protect their critical assets.

A systematic analysis of potential security threats involves a series of steps aimed at identifying potential security risks, assessing their impact, and determining the optimal course of action to mitigate them. It is important to collect all the necessary data and information to fully understand the problem.

The collected data and information must be analyzed to determine the root cause of the problem. It is important to consider all possible solutions, identifying their pros and cons.

It is important to consider factors such as the feasibility, cost and potential impact of each decision. This is followed by the implementation of the selected solution and monitoring of its effectiveness over a certain period of time. By following these steps, organizations can effectively use systems analysis to identify and prevent potential security threats.

An ISO 27001 compliance audit aims to review an organization's security policies, evaluate access controls, and ensure compliance with regulations to improve security. This is essential for businesses that must comply with industry regulations, as failure to comply can result in fines and loss of customers.

Many companies view ISO as a badge of prestige, as it is the world's largest set of recognized business principles, and more than a million companies worldwide have some form of ISO certification. ISO 27001 standards are specifically designed to protect confidential user information, and compliance with them is an example of compliance auditing. But, the use of technology (firewalls, antiviruses and backups) does not guarantee complete protection against data leaks and operational problems.

This has to do with how people use these security tools, procedures and protocols. ISO 27001 standards address this issue by requiring systems to identify risks and prevent security incidents.

A risk-based approach is an assessment of information security risks based on threat analysis and technical, legal, financial and organizational risks. Continuous improvement is about updating, adjusting and improving the system in response to changing conditions inside and outside the organization. The PDCA cycle is used for management and allows the system to be assessed and improved in accordance with the ISO 27001 standard.

Information Security Management involves documenting policies, procedures and practices and systematically measuring the effectiveness of these processes. A company can declare its compliance with ISO 27001 after receiving certification from an independent certification organization. This confirms that it meets all the requirements of the information security management standard. System security analysis involves looking at the entire system, not just individual components or vulnerabilities. This approach is especially useful in identifying hidden or complex security risks that would not otherwise be detected.

To use systems analysis for security purposes, it is important to follow several key steps: identify all components of the system, from hardware and software to human and cultural elements; assess how system components can be used by hackers; determine how system components interact with each other and how threats can spread throughout the system.

Based on the risk and vulnerability analysis, mitigation strategies and solutions can be developed to address the issues identified by the analysis.

Systems analysis can be used to analyze databases to identify vulnerabilities and security threats. For example, to detect SQL injections, you can analyze the SQL code used by the application to access the database. One possible way to process malicious SQL code:

System analysis can help identify vulnerabilities in a company's information system. To do this, you can analyze the architecture of the system and its components. For example, you can check whether the system complies with security standards such as HIPAA or PCI DSS.

HIPAA (Health Insurance Portability and Accountability Act) is a piece of legislation passed in the United States in 1996 that regulates the processing, storage and transmission of health information (Protected Health Information (PHI). HIPAA contains security standards that are required by all healthcare organizations and companies that handle patient medical data in the United States.

HIPAA security standards include requirements to protect the confidentiality, integrity, and availability of health information. They cover the following areas: requirements for access restrictions to premises where medical data, CCTV cameras, access control devices, etc. are stored; requirements for the protection of electronic medical data, including data encryption, access control and log auditing; requirements for documentation of medical data processing procedures, employee training and audits.

System analysis can be used to analyze application code and identify potential security threats. For example, when processing input data, the application must check for correctness and filter out malicious code. System boundaries may include the order management system, customer data storage, and payment gateways. These system components are important safety assets.

Once potential threats have been identified, the system must be examined to identify specific vulnerabilities. For example, unsecured access points or outdated security protocols may be vulnerable.

The final step is to develop a plan to address each vulnerability. Various security measures can be implemented to reduce risks, including the introduction of new technologies, updates to security protocols, training of personnel on best practices, etc. For example, a company may decide to protect data with two-factor authentication or use better security software solutions.

Systems analysis helps identify and evaluate potential cyber security risks, providing insight that allows decisions to be made to strengthen security protocols. Using system analysis helps identify any potential security breaches. Systems analysis can take many forms, from a comprehensive security risk assessment to a formal security program assessment. Regardless of the form, using the right tools can help identify systematic security weaknesses, keeping the organization safe.

A security incident capture system (SIEM) is used to collect and analyze data from various sources to identify security threats. SIEM can be used to detect malicious activities, network attacks, and security policy violations. Examples include Tripwire, Nagios, SolarWinds and AlienVault software.

CISM software is used to assess security threats, identify vulnerabilities, formulate risk management plans, and remediate vulnerabilities. Examples of CISM software include SecurityMetrics, IBM QRadar, and Symantec Control Compliance Suite.

Security audits are used to identify threats and assess risks, and to ensure compliance with security regulations and policies. Examples of security auditing software include Qualys, Nessus and OpenVAS. Checking the security of web applications for vulnerabilities is carried out using OWASP ZAP, Acunetix and Burp Suite tools. User access monitoring can be implemented using Active Directory, LogRhythm, Splunk and Netwrix. Indicators of compromise are used to detect the presence of hackers on a network. Indicators of compromise help detect the presence of malware and other anomalous activity on the network. Examples of indicators of compromise include McAfee Threat Intelligence Exchange, IBM QRadar, and Cisco Stealthwatch.

During the COVID-19 pandemic, many organizations were forced to switch to remote work. To improve the remote work process, tools such as Zoom have been developed, which are used to create virtual conferences and video calls. This has allowed organizations to continue their work online, ensuring their workflows are efficient and secure. However, as is the case with Zoom, remote work apps can also be compromised and subject to security breaches.

User data, including login information, email address, meeting URLs and host keys, can be used by criminals to access meetings and for other fraudulent activities. Data compromise can result in legal claims from employees and fines from regulators in most countries. To prevent such incidents in the future, organizations need to implement extensive information security programs, as well as regularly train employees in the rules of working in an online environment.

Security audits and systems analysis can help organizations identify vulnerabilities and improve security controls, which can help prevent future security breaches and protect customers' personal data.

COMPUTER VIRUS

A computer virus is a program that can create copies of itself it introduces them into the resources of computer systems and networks. It also performs actions without user intervention.

The virus infects other programs and also carries out planned destructive actions. To disguise itself, the virus is not always activated, but only when certain conditions are met (time, action). After the virus performs the actions it needs, it transfers control to the program in which it is located.

Like real viruses, computer viruses hide and multiply. Viruses perform various destructive actions. They display annoying text messages; create sound effects; create video effects. They slow down your computer, gradually reduce the amount of RAM and increase hardware wear; cause failure of individual devices, freezing or rebooting of the computer.

They simulate repeated operating system errors; destroy the FAT table, format the hard drive, erase the BIOS, erase or change settings in CMOS, erase sectors on the disk, destroy or corrupt data, erase anti-virus programs. They

carry out scientific, technical, industrial and financial espionage; disable information security systems and give hackers secret access to a computer. They make illegal deductions from every financial transaction.

The main danger of self-replicating codes is that virus programs begin to live their own lives, practically independent of the program developer. The main symptoms of a computer virus infection are the following:

- slowdown of some programs; increasing file sizes;
- the appearance of previously non-existent files;
- reducing the amount of available RAM;
- the appearance of malfunctions in the operating system;
- writing information to disks at times when this should not happen.

According to the classification of viruses, network viruses are distinguished, distributed by various computer networks. File viruses infect executable files with the extension exe and com.

This class also includes macro viruses written using macro commands. They infect non-executable files in Word and Excel.

Boot viruses are embedded in the boot sector of a disk or in the sector containing the system disk boot program. Some viruses write to free sectors of the disk, marking them as bad in the FAT table. Boot-file viruses integrate features of the last two groups.

A resident virus can be divided into two parts - the installer and the resident module. When an infected program is launched, control is gained by the installer, which places the resident virus module on the system and performs the operations necessary to ensure that the latter is stored there permanently; overrides some interrupt handlers so that the resident module can take control when certain events occur.

Non-resident viruses do not infect RAM and are active only once when the infected program is launched.

Non-dangerous viruses create sound and video effects. Dangerous viruses destroy some of the files on the disk. Very dangerous viruses format the hard drive on their own.

Companion - viruses do not change files. They create new satellite files (duplicates) for exe files, having the same name, but with the extension com. The com file is detected first, and then the virus launches the exe file.

When spreading copies of themselves parasitic viruses necessarily change the contents of disk sectors or files. These include all viruses except companions and worms.

Worms (replicators), like companions, do not change files and disk sectors. They penetrate a computer over a network, calculate the network addresses of other computers and send copies of themselves to these addresses. Worms reduce network bandwidth and slow down servers.

Invisible people (stealth) use a set of means to disguise their presence on a computer. They are difficult to detect. They intercept calls from the operating system to infected files or sectors and substitute uninfected sections of the files.

Polymorphs (ghosts, mutants) encrypt their own body in various ways. They are difficult to detect. Their copies contain practically no completely matching sections of code. The Trojan program disguises itself as a useful or interesting program, while also performing destructive work during its operation.

It collects information on the computer that is not subject to disclosure. Unlike viruses, Trojan programs do not reproduce independently.

A virus program can function as a single unit. It can also be divided into parts. These parts contain instructions that indicate how to put them together to recreate the virus.

Antivirus programs are developed to combat viruses. This is a software product or device that performs one or more of the following functions:

1) protecting data from destruction;

2) virus detection;

3) neutralization of viruses.

Detector programs are designed to detect specific viruses known in advance to the program and are based on comparing a characteristic sequence of bytes (signatures) contained in the body of the virus with the bytes of the programs being scanned. Detector programs are equipped with heuristic analysis blocks. In this mode, an attempt is made to detect new or unknown viruses using code sequences characteristic of all viruses.

Disinfector programs (phages) not only find infected files, but also treat them by removing the body of the virus program from the file. Auditor programs analyze the current state of files and system areas of the disk and compare it with information previously saved in one of the auditor files. The status of the boot sector, FAT table, as well as the length of files their creation time, attributes, and checksums are checked.

Filter programs (monitors) notify the user of all attempts by any program to perform suspicious actions. Filters control updating program files and the system area of the disk, and formatting the disk.

When working on a network, a filter program must be installed. Before reading information stored on other computers from floppy disks, you should always check those floppy disks for viruses. When transferring files in archived form, you must check them immediately after unzipping.

When working on other computers, you need to write-protect your floppy disks. Make archival copies of valuable information on other media. Do not leave the floppy disk in the drive when turning on or restarting the computer, this may lead to infection with boot viruses.

If you receive an email with an executable file attached, you should not run the file without first checking it. It is necessary to have an emergency boot floppy disk from which you can boot if the system refuses to do so normally.

DEFINITION OF CLOUD SECURITY

Cloud security is a set of policies, controls, and technologies to protect data, applications, and infrastructure services. All of these components work together to help keep your data, infrastructure, and applications secure. These security measures protect the cloud computing environment from external and internal threats and cyber security vulnerabilities.

As enterprises accelerate digital transformation (DX) initiatives, aggressively redesign operations, and reimagine entire business models using cloud services, such widespread adoption is also creating new opportunities for cyber criminals to commit cyber fraud.

As these organizations move to digitally transform their operations so quickly, there is often little time to think about effective security controls. Businesses often choose not to apply proven best practices, making it difficult (if not impossible) to accurately assess and manage risks.

As businesses adapt to constant change and actively move to the cloud, there is a need to unify disparate views and agendas into a cohesive strategy. Organizations that view the move to the cloud as an opportunity to actively cultivate a security-first strategy will have to balance ensuring cloud services are usable while protecting sensitive transactions and data.

The benefits of cloud security involve the use of artificial intelligence (AI) and machine learning (ML) to automatically adapt to and mitigate security threats; Leverage autonomous capabilities to scale response, mitigate risk, and mitigate security failures.

Proactively protecting data through access controls, managing user risk and transparency, and providing tools for analysis and classification are expected; Apply a shared responsibility model for cloud security to intelligently address security efforts along the customer-cloud provider journey; Integrating security features into the architecture design to achieve a “security first” approach. Cloud security provides organizations with an approach to solving security problems and ensuring compliance with regulatory requirements.

Effective cloud security requires multiple layers of protection across the cloud technology stack, which includes proactive controls designed to block authorized access to sensitive systems and data; detective controls, designed to detect unauthorized access to systems and data and their changes through auditing, monitoring and reporting; automatic controls designed to prevent, detect and respond to security updates, both routine and critical; administrative control, designed to monitor the application of security policies, standards, practices and procedures.

Machine learning and artificial intelligence can complement the cloud security portfolio with context awareness technologies. Cloud security enables enterprises to protect IaaS, PaaS and SaaS by extending protection to the network, hardware, operational, application, silicon and storage layers.

Cloud cloud security is the shared responsibility of security between the cloud provider and the customer. The shared responsibility model for cloud security is a basic design for managing security and risk in the cloud, allowing for the division of responsibilities between the cloud service provider and the subscriber. A clear understanding of the shared security responsibility model for all types of cloud services is critical to cloud security programs.

Unfortunately, it can also be said that the shared security responsibility model is one of the least understood cloud security concepts. In fact, when compared to a cloud service provider (CSP), only 8% of CISOs fully understand their role in SaaS security.

The shared security responsibility model defines the cloud service provider's responsibility for ensuring the security and availability of the service, as well as the customer's responsibility for ensuring the secure use of the service, with each having specific responsibilities.

Failure to adequately protect data can have serious and costly consequences. Many organizations that suffer the consequences of a breach may not be able to absorb the costs, and even large companies may feel the impact on their financial performance. The point of the Shared Security Responsibility model is to provide flexibility with built-in security capabilities that enable rapid system deployment. Therefore, organizations must understand their responsibilities for cloud security: this is commonly referred to as security “from” the cloud and security “in” the cloud.

Enterprises are offered a wide range of cloud security tools to ensure security when moving workloads and data to the cloud. However, some of these tools come with custom instructions and are offered as separate services. Cloud users and administrators must understand how cloud security services work, how to configure them correctly, and how to maintain deployed cloud solutions. While there is no shortage of different security systems available today, they can be difficult to set up and it can be easy to make mistakes in one area.

The ongoing risk of phishing and malware, growing cyber fraud and a range of misconfigured cloud services are putting even more pressure on cyber security programs that address complex challenges. As a result, organizations face data breaches, which entail brand damage, recovery costs and fines.

Trust is paramount when choosing a cloud partner who will be responsible for their part of the overall security model. Organizations must clearly understand their roles and responsibilities, and have access to independent third-party security audits and certifications.

Complex threats require new, modern security solutions that can predict, prevent, detect, and respond to threats using machine learning.

Multi-layered security across the technology stack must include proactive, detective, and administrative controls over the appropriate people, processes, and technologies to ensure the security of cloud service data centers.

As mobile devices, apps, and user information become more widely used, accounts become the new perimeter. Controlling access and privileges in the cloud and on-premises systems is critical.

A cloud access security broker and cloud security management solution increases visibility and control over an organization's entire cloud environment.

Regulatory compliance is a must, but compliance and security are not the same thing. Organizations can violate regulatory requirements without compromising security, for example through configuration changes and errors. It is critical for companies to have a cloud management solution that provides complete, timely, and actionable compliance data across all cloud environments.

The cloud provider should enable security controls by default rather than requiring the enterprise to remember to turn them on. Not everyone has a clear understanding of the various security controls and how they work together to reduce risk and risk. For example, data encryption should be enabled by default. Clouds must have consistent controls and data protection policies.

To ensure workload security, security policy administrators should configure and enforce security policies for cloud users and partitions. A unified view of all cloud security controls across all cloud users is also necessary to detect resource configuration errors and insecure activities across all users, giving security administrators the ability to monitor and resolve cloud security issues.

The principles of separation of duties and least privilege access are practical security guidelines that should be applied in cloud environments. This ensures that individuals do not have excessive administrative rights and cannot access sensitive data without additional authorization.

As cloud adoption continues to accelerate as a result of digital transformation priorities, companies must anticipate and navigate the complexities of securing their cloud environments. It is very important to choose a cloud service provider that can develop a security system that is automatically built into the entire cloud technology stack (IaaS, PaaS, SaaS).

When considering the prospects for the development of cloud security, the security of the cloud infrastructure is relevant: protecting workloads using a “security first” approach, focused on the security of computing, networks and storage systems of the cloud infrastructure, starting with its architecture. Apply core security services to ensure your most critical business workloads are secure.

Cloud database security involves reducing the risk of data leakage and accelerating regulatory compliance in the cloud. Implement database security solutions including encryption, key management, data masking, privileged user access control, activity monitoring and auditing.

Cloud application security is seen as protecting mission-critical applications from fraud and misuse is absolutely essential to protecting a company's critical business data. Granular access control, visibility and monitoring are key components of modern multi-layered defense.

Corporate security and privacy is defined as protecting the confidentiality, integrity, and availability of data and systems hosted in the cloud, regardless of the cloud product selected. As security teams move to cloud and multi-cloud environments, they are faced with a growing attack surface, alert overload, and a lack of cybersecurity skills. To solve these problems, advanced services from the cloud service provider are used to control access to data, such as access to specific resources using secure credentials, regardless of whether they are hosted in the cloud or on-premises.

SECURITY MANAGEMENT

In the general definition, safety is understood as the state of an object's protection from the harmful effects of the external or internal environment. Safety management takes on the function of checking and regulating compliance with the rules of safe operation of the company, both in the production and service sectors. The development and implementation of this concept is carried out by specialists who are highly qualified in the issues presented, which allows them to competently draw up and subsequently comply with the requirements of the safety rules of the enterprise in the selected market.

Enterprise security management refers to a coordinated and systematized set of actions and methods aimed at optimally managing risks and associated potential threats and other impacts. Achieving this concept in a modern company is possible only with the precise formulation of specific tasks. The development of safety rules should also be carried out by qualified specialists and responsible representatives of the company.

The main priority at the stage of implementing security management is to ensure that all employees of the company are interested in strict compliance with the prescribed rules and recommendations.

In this case, a high degree of safety of technical operations (production of finished products and provision of services) is achieved; commercial transactions (buying, selling and volume); financial transactions (raising finance and further disposing of it).

A high degree of insurance operations is also achieved (insurance, protection of life and health of personnel and company property); accounting operations (accounting, accounting, statistics and costing).

A similar level is provided for administrative operations (anticipation, organization, control and coordination).

Each of these operations can serve as a source of danger, both due to its incorrect execution and as a way for hackers to penetrate the structure of the organization. Threats considered by the concept of security management within a company are classified as temporary or permanent, and external or internal. Security theory identifies threats associated with competition, human factors, crime, man-made and natural factors.

In business activities, the main types of threats are divided into physical and economic threats. Each of them is also divided into subspecies, considered separately in each case.

The creation of an effective company security system and its maintenance should be based on the scientific achievements of security theory.

The purpose of such a system is the timely identification and prevention of external and internal threats to a business that may interfere with its further development and viability. Also, the most significant functions of a security system are identifying real and predicting potential threats; applying methods to eliminate them, as well as eliminating the consequences; selection of tools and tools aimed at improving the enterprise security system; creation and provision of a protected environment for enterprise employees that allows them to safely perform their duties.

A security strategy must be clearly developed that allows the company to achieve its most important objectives in terms of creating and maintaining a safe and competitive environment within the organization. Thanks to this, each employee can safely and effectively demonstrate their professional abilities and climb the career ladder.

The structure must clearly define the subjects and objects of the security system. They are interconnected elements combined into a system that provides a safe environment for the operation of the enterprise. System objects are the elements on which all security efforts are directed. These include administrative services, purchasing departments, production sector and commercial departments. Subjects are responsible departments of the enterprise that are directly involved in the creation and modernization of the security system.

The information security management system is part of the overall management system, based on the use of business risk assessment methods for the development, implementation, operation, monitoring, analysis, support and improvement of information security.

An ISMS includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

The standard establishes requirements for the development, implementation, operation, monitoring, analysis, support and improvement of an organization's documented business risk information security management system.

The standard establishes requirements for the implementation of information security management and control measures that can be used by organizations or their departments in accordance with established goals and objectives for ensuring information security.

As a result, we achieve: protection of information assets and guarantee of stakeholder trust; ensuring the possibility of authorized timely receipt of accurate and complete information; meeting the safety requirements of clients and other interested parties; improving the plans and actions of the organization; compliance with the organization’s information security goals; integration with relevant requirements of other management systems; facilitating continuous improvement and adjustment of current organizational goals and external conditions; understanding the information security requirements of the organization and the need to establish information security policies and goals; implementation and use of control measures to manage the risks of the organization’s business risks; increasing assurance that information assets are sufficiently protected on an ongoing basis from information security threats.

ETHICAL EGOISM

Ethical egoism is the idea of pursuing one's own interests, as well as the complete exclusion of the responsibilities of protecting someone else's interests.

We are talking about a normative (prescriptive) theory concerning the moment of human behavior. Ethical egoism differs significantly from the theory of psychological egoism, which notes that any actions of people ultimately pursue self-interest.

Arguments supporting ethical egoism are based on the idea that anyone who is committed to self-interest participates in promoting the common good. The result is achieved through people acting as the best judges of their own interests. People are much more motivated to work hard for themselves than to achieve other results. However, there is an obvious objection that the argument does not support ethical egoism.

Ethical egoism is unable to provide solutions when a problem arises involving a conflict of interest. Ethical egoism excludes any attempt to remain impartial. People are left to distinguish between themselves and all other people and provide preferential treatment for themselves.

Many perceive this as a contradiction to the very essence of morality. The golden rule of different versions says: people should treat each other based on their own wishes in the relationship.

ANONYMITY ON SOCIAL NETWORKS

Many people want to achieve anonymity on the Internet. There is a secret of personal life and a secret of correspondence - you want to protect them. The bad news is that providers and Internet services are often willing to neglect the rights of their users in search of commercial profit. In addition, information can get to hackers. Anonymity can be called a state when it is impossible to compare an action on the network and the individual who performed this action. For a specific person, it is impossible to compile a list of his online activities.

It is impossible to ensure complete anonymity on the Internet - a digital trace remains. Given sufficient resources, it will lead to a real person. But for an ordinary person, not a cybercriminal, it is enough to follow a few rules that will make him almost incognito.

Data is transmitted in clear text by default. A hacker, having received network traffic, will be able to see all the data transmitted in it. To avoid such a threat, many sites use crypto protocols for data transmission. The main protocol on the Internet is HTTP. Its version that supports encryption is called HTTPS. HTTPS is a standard that allows you to protect the transmitted data between the site and the user. It is used by almost all significant services and sites.

The IP address is still the primary user identifier on the network. Now access is provided only after identifying a person using a passport, so the provider will always be able to tell who exactly was working at a certain point in time using an IP address.

To hide an IP address, they mainly use a VPN tunnel, which allows you to encrypt traffic and hide it from your Internet provider. If you use a VPN service, all traffic will be available to its owners. It is worth choosing services with a proven reputation. You also need to be prepared for the fact that the VPN service will most likely be paid.

TOR uses so-called onion routing, when at each section of the network a data packet is encrypted over the previous packet and then decrypted in reverse order. By analogy with a VPN, traffic is released onto the Internet in some other place, but not at just one, but at many exit points, which significantly complicates access to it and its analysis.

In addition to anonymous access to regular sites, the TOR project is used to organize the darknet. The speed of your Internet connection via TOR will be significantly slower than usual. But you can maintain anonymity on the Internet.

When working with digital platforms, files are created on the computer in which the site stores information during and between sessions of working with them - cookies. They save user settings to simplify working with the resource and improve many services. For example, in order not to enter a password every time, the site establishes an authorized session and stores its identifier in a cookie. The lifetime of cookies can be limited.

In order for the site to recognize the user, you need to either delete his cookies through special browser plugins, or use “Incognito” mode to log in. Unlike regular cookies, third-party cookies are created by websites. These cookies are set by Facebook's "Like" buttons and services from internet giants. These cookies can later be read by Facebook itself. The algorithm uses this information to show targeted advertisements in the news feed.

To remain anonymous regarding third-party cookies, you can use the “Incognito” mode in your browser or special plugins that block “Like” buttons and similar “bugs” on sites. But if blocked, problems often arise with displaying content, since some useful functionality is blocked along with the tracking block. By default, sites have access to a very limited amount of information about the user’s end system, his computer. For example, the MAC address, the unique number of the user’s network card, is unavailable. The processor serial number also remains unavailable.

However, some things are still available: browser and operating system version, screen resolution, time zone, installed language and browser extensions, and similar little things. Do not underestimate this set of information. The vector made up of these parameters will be unique. The site can remember the impression and then compare it every time you enter the site.

To protect against this and ensure complete anonymity on the Internet, special browser plugins are installed that will return a randomly generated snapshot when requesting sites.

To protect against this and ensure complete anonymity on the Internet, special browser plugins are installed that will return a randomly generated snapshot when requesting sites.

There is another method - behavioral analysis. The essence of the method comes down to analyzing mouse movements and the user's keyboard handwriting. Keyboard handwriting is the way a person types text. Micro pauses between different symbols are a unique value. The complexity of the method lies in the fact that each time you need to wait for typing or a sufficient amount of mouse movement to carry out the analysis.

CYBER CRIME

Cyber crime is illegal activities carried out by people using information technology for criminal purposes. The main types of cyber crime include the distribution of malware, password hacking, theft of credit card numbers and other banking details, and the dissemination of illegal information via the Internet.

The main features of computer crimes were formulated in 1974 at the Conference of the American Bar Association.

Three areas of computer crimes have been identified: using or attempting to use a computer, computer system or network of computers for the purpose of obtaining money, property or services; intentional unauthorized action aimed at changing, damaging, destroying or stealing a computer, computer system, network of computers or software systems, programs or information contained therein; intentional unauthorized disruption of communications between computers, computer systems or computer networks.

Unauthorized access is carried out using someone else's name, changing the physical addresses of technical devices, using information remaining after solving problems, modifying software and information, stealing a storage medium, installing recording equipment connected to data transmission channels

A “time bomb” is a type of “logic bomb” that goes off when a certain point in time is reached. The Trojan horse consists of secretly introducing commands into someone else's program. They allow you to implement new functions that were not planned by the owner of the program, but at the same time maintain the same functionality.

Viruses pursue the hacker's goal to erase all program data, move on to the next computer program and do the same. They have the ability to move through communication networks from one system to another system. They spread like a viral disease. The virus is not detected immediately. At first, the computer harbors an infection, since the virus is often used in combination with a “logical bomb” or “time bomb” to disguise itself. The virus monitors all processed information and can move using information transfer.

Text-based antivirus programs are used against viruses. Security programs are divided into three types: filtering (preventing the penetration of the virus), anti-infective (continuously monitoring processes in the system) antiviral (set to detect individual viruses).

A feature of computer negligence is that, in principle, there are no error-free programs. If a project in almost any field of technology can be completed with a huge margin of reliability, then in the field of programming such reliability is conditional, and in some cases almost unattainable.

Forgery of computer information is a type of unauthorized access with the difference that it can be used, as a rule, not by an outside user, but by the developer himself, who is quite highly qualified.

The idea of the crime is to falsify the output information of computers in order to imitate the performance of large systems of which the computer is an integral part. If the counterfeit is done cleverly enough, it is often possible to deliver obviously faulty products to the customer.

The appropriation of machine information, including software, through unauthorized copying does not qualify as theft, since theft involves the seizure of valuables from the organization's funds. In the event of unauthorized access to property, machine information may not be removed from the funds, but copied. Information should be identified as an independent subject of criminal legal protection. The word hacker (originally someone who makes furniture with an ax) has several definitions:

1) A person who likes to explore and extract the maximum capabilities of programmable systems, unlike most users who do not go deeper than the required minimum.

2) Someone who programs passionately, even obsessively, or enjoys the development process more than programming theories.

3) A person who is able to quickly grasp the essence of a phenomenon.

4) A person capable of rapid program development.

5) An expert on a particular system, usually using it frequently.

6) Expert or enthusiast of any kind.

7) One who experiences intellectual pleasure from creatively overcoming or circumventing limitations.

8) A person who tries to discover the necessary information

The modern concept of "hacker" characterizes all network hackers and creators of computer viruses. Types of hackers:

Cracker - deals with hacking application software in order to obtain full-fledged commercial versions from shareware programs (programs with limited functionality, intended mainly to demonstrate to the user the capabilities of the full version). Kraker is a fairly high-level programmer.

Fricker - explores telephone networks in order to find opportunities to call for free. Historically, phreaking is the very first type of hacker activity, which arose in the 60-70s of the 20th century. In recent years, phreakers have also begun to explore networks for mobile phones.

Carder - is engaged in illegally obtaining credit card numbers and information about their owners. Often this activity is combined with hacking activities. Carding is considered the most serious crime and is therefore the most dangerous type of hacking activity.

Recently, only email viruses that spread due to errors in the Outlook email program have become widespread, and the search for such errors can be considered hacker activity.

The main goal of Internet fraud is to deceive users of the global web and steal confidential information, which is then used for the personal purposes of the criminal. As a result of such activities, millions of people around the world suffer significant losses every year.

There are many different types of Internet fraud. But they all have one thing in common: the success of all these methods directly depends on the degree of gullibility and carelessness of the user.

You need to follow a few simple rules: do not trust all incomprehensible messages that ask you to provide personal data; ignore spam; do not open suspicious emails; do not disclose personal information; be careful when making online purchases, choose sites that ensure the security of transactions and the confidentiality of personal data.

It is necessary to use a multi-level security system. To do this, you need to install and regularly update computer security programs (antivirus and firewall).

On a social network there is always a risk of encountering harmful information that encourages drug use, suicide, information about pseudo-religious and mystical activities and sects.

On the network you can come across various services that are offered after payment to a short number. Most often this is a simple scam. Therefore, you should not accept files from strangers or open dubious links, because this can infect your computer with viruses.

Propaganda of violence, prohibited ideas, and distribution of pornography takes place on social networks. Despite monitoring and blocking of such pages, they appear again and do their best to hide their purpose. The possibilities of the Internet are used by representatives of extremist movements.

A remote attack or exploit is aimed at capturing data, infecting networks with virus software, and causing significant damage to the network and individual computers. Depending on the techniques used, several types of remote attacks can be distinguished: DNS cache corruption, TCP desynchronization, DoS attack, ICMP attack and port scanning.

Due to the variety of remote attack tools, there are many ways to protect against them. Given the scope of technical means, a sufficiently large group of hackers will always be able to find a gap in the system.

A client-side attack relies on interaction with a network or computer user. Hackers try to trick the user into entering their details on a fake (phishing) site. All available methods are used: malicious links, documents and applications. Even an experienced user cannot always distinguish a phishing site from the original one - the copies are plausible, and it is very difficult to notice a minor typo in the site address.

Hackers are very patient and are ready to wait for months until the user, through his actions, gives them access. Therefore, all employees must be aware of this danger and understand the responsibility they take on. Corporate computers should be used only for business purposes, and the amount of software on them should be kept to a minimum, only authorized programs should be used.

Reducing possible breach points through browsers, email clients, applications and media players is a great method for preventing hacker attacks.

The brute force method is used by hackers when none of their attempts to gain access to a network using standard methods have been successful. The essence of the method is to use all known penetration methods in the hope that one of them or a successful combination of methods will allow one to crack the security system. Often, a complete search of the values of fields (for example, addresses and passwords) is used until the correct option is selected.

This type most often causes a lot of damage to the network and equipment, but it can be easily tracked by large amounts of unknown data that appear on the network.

To protect against online brute force attacks, use a limited number of password entry attempts, a delay between entry attempts, special password recovery questions, the use of CAPTCHA or SMS verification, and account blocking after several unsuccessful login attempts.

Social engineering involves psychological manipulation. If successful, the user voluntarily transfers confidential information to the hacker: phone numbers, addresses, passwords, credit card numbers, etc. Sometimes this is the simplest and most effective method of gaining access to a well-protected network (this is how Edward Snowden gained access to the US NSA network).

Man in the Middle is the interception and spoofing of messages between two users. The attack uses unprotected data transfer protocols and in almost 100% of cases, users have no idea that their messages are being intercepted, and hackers control the entire communication process.

You should pay attention to the settings of the router and server, use strong encryption and secure data transfer protocols, install browser plugins that automatically encrypt outgoing information and avoid access via public Wi-Fi.

Hackers are getting smarter every day. Attacks have evolved from short and aggressive attacks to methodical, well-planned, long-running operations involving several (if not all) hacking methods.

Traditional methods of protection (antivirus, firewalls, VPNs, password managers, traffic monitoring, Internet gateways and work in a dedicated perimeter) serve primarily to track the first steps of hackers on the network. Hackers understand all possible types of protection as well as, and often better than, security specialists, so all modern penetration methods are designed by default to bypass the protection of corporate systems.

A large number of cyber attacks are successful for several reasons. They do not depend on the location of the cyber criminal and the distance from him of the potential victim, as well as time frames and time zones. A hacked IT environment can have critical consequences for the business: causing reputational damage and reducing the level of trust on the part of customers, because their data can also fall into the wrong hands. Infrastructure hacking is also associated with financial risks: due to the outflow of customers and the loss of the organization’s unique innovative developments, its competitiveness may significantly decline in the market.

The situation is complicated by the fact that the methods and tactics of attackers are constantly evolving. Hackers are constantly adapting their attacks to new realities and technologies. Modern cyber attacks are highly automated, which allows hackers to speed up their implementation and use artificial intelligence to increase the success of their implementation. The security measures used effectively fulfill their task of ensuring security. They block standard attacks, but they are not yet perfect against targeted, manual threats.

Hackers' actions can be divided into two main types - distributed and targeted attacks. Distributed cyber attacks are the use of a botnet and are aimed simultaneously at a large number of users and company resources. Such attacks use leaked databases of organizations and users.

Targeted attacks are a pre-planned attack on a specific company or infrastructure. In these incidents, the hacker not only gains access to internal resources, but also remains on the company network until he is detected. This could be days, months and even years. Targeted attacks are carried out by hackers with high technical competence. They use automated tools independently determine attack vectors exploit 0-day vulnerabilities and some system features, based on their experience.

Cyber attacks pose a danger to both ordinary users and businesses. In both cases, the consequences can be not just unpleasant, but also critical. DDoS attacks, phishing and video conferencing attacks topped the list of cyber threats. However, other types of attacks also bring a lot of problems to both businesses and ordinary users.

Hackers blackmail users of instant messengers using bots, break into the network through QR codes and exploit vulnerabilities in the settings or encryption of a legitimate network, and also resort to “brute force” attacks. In order to better understand the actions of hackers, you need to know what types of attacks on infrastructure exist and their key features.

DDoS attacks are distributed denial of service attacks. They are implemented through the use of several compromised computer systems as sources of attack traffic. These attacks clog systems with large numbers of requests, causing throughput to decrease and systems to become overloaded and unavailable.

Phishing attacks rely on emails that can be disguised as legitimate messages from various companies. In such a fake message, hackers may offer to follow a link, download an infected file, or ask to transfer confidential user data - logins, passwords and bank card account numbers.

Brute-force represents "brute force" attacks. They are a fairly simple method of infiltrating infrastructure and involve “guessing” user accounts. Some hackers use applications and scripts as brute-force tools that try many password combinations to bypass authentication processes. If the password is weak, it will only take a couple of seconds for hackers, so the business should have a strict password policy.

A bot is a software robot that imitates or replaces human behavior and performs simple tasks at a speed that exceeds user activity. Some bots are useful and their actions are aimed at supporting users, but there are also malicious ones. For example, they are used to automatically scan websites and find vulnerabilities, as well as carry out simple cyber attacks.

In a man-in-the-middle (MITM) attack, the cybercriminal becomes the third wheel and passes all web traffic through himself. At this point, the potential victim is unaware of anything, which leads to the fact that all login credentials for the systems are in the possession of the hacker.

The information obtained can then be used to steal corporate data or make unauthorized transfers of funds.

ENVIRONMENTAL SAFETY COMPONENTS

This or that manifestation of security is interconnected with the nature of dangerous changes in the environment, thereby forming an unstable worldview among individuals, social groups and modern society. Following this logic, it turns out that if there were no dangers in the natural world then there would be no problems associated with ensuring safety.

Security represents a specific, well-defined result of specific activities to neutralize, prevent threats, and ensure protection. From this thesis follow two approaches to understanding the nature of security: as a manifestation of the objective nature of living systems to maintain their integrity due to stable or unstable interaction and state; as a subjective natural defensive reaction or activity to create a certain environment for one’s self-preservation.

Safety is a qualitative systemic property of organic life, which not only ensures the survival of various organisms, but also contributes to their development. The main goal of any of these living structural levels is its own survival by creating a safe environment of existence.

The problem of social security has a universal character in the system of philosophical knowledge. This is due to the following reasons:

All spheres of human activity are to a certain extent related to the safety factor. Some of them act as the most important determinants of social security. Others appear as consequences of social actions and processes aimed at ensuring security in one form or another.

Society appears in the form of a subsystem of objective reality, relatively isolated from natural formations, but organically connected with them. It obeys the universal laws of existence.

Characteristic of society, the social form of movement, as a prerequisite for its existence, relies on the lower forms of movement of matter (mechanical, physical, chemical and biological) and contains them within itself. This indicates the importance of the natural foundations of social security, without which the very existence of society becomes impossible.

The main difference between society and other subsystems of objective reality is that it always represents a certain combination of material and ideal, objective and subjective, spontaneous and planned, random and natural. This is due to the fact that in society, unlike nature, people act who are endowed with consciousness and will; their actions are always purposeful.

But activity people does not always lead to the expected results, since in complex social phenomena there is a clash of forces, actions, and actions of various subjects, which determines the objectivity of the general course of the social process. Such objectivity of the patterns of functioning and development of society is one of the most important determinants of social security.

Safety as a state of preservation involves maintaining a certain balance between the impact on environmental objects.

Distributed network attacks are often called Distributed Denial of Service (DDoS) attacks. This type of attack uses certain bandwidth limitations that are typical for any network resources, for example, the infrastructure that provides conditions for the operation of a company's website.

A DDoS attack sends a large number of requests to the attacked web resource in order to exceed the site's ability to process them all... and cause a denial of service. In simple words, this is an attack on a computer system with the aim of bringing it to failure that is, creating conditions under which bona fide users of the system cannot access the provided system resources (servers), or this access is difficult.

Currently, DoS and DDoS attacks are popular because they allow almost any system to fail. Usually the attack is organized using Trojan programs. Trojans first infect insufficiently protected computers of ordinary users and may not manifest themselves on the infected computer for quite a long time, waiting for a command from their owner. A computer can be subject to such an attack when visiting various infected sites, receiving email, or installing unlicensed software.

When the attacker is about to launch an attack, he issues a command, and all previously infected computers begin simultaneously sending requests to the victim site. The most massive DoS attack in Belarus was carried out by extremist channels in 2021.

The attackers, deliberately concealing information about criminal liability for participation in a DoS attack, attracted more than 10 thousand citizens (mostly young people) to participate in it. Almost all participants in this illegal action were identified, and the most active of them were brought to criminal liability.

IT LANDSCAPE SECURITY TOOLS

A competent choice of IT landscape security tools is the key to maintaining the confidentiality and safety of corporate data. Information security measures can be divided into three key types: technical means, organizational measures and preventive security checks.

Let's consider technical means. A WAF complex is a firewall for web applications, the main functions of which are to detect and block attacks. Using a WAF complex, you can not only detect malicious traffic, but also determine which attacks were aimed at business-critical systems. The implementation of this tool allows a business to protect itself from attacks on the business logic of applications.

Firewalls (FW) are a digital security barrier around IT infrastructure that protects the network and prevents unauthorized access. Firewalls provide network security by filtering incoming and outgoing network traffic based on a set of rules. The purpose of firewalls is to reduce or eliminate the occurrence of unwanted network connections while allowing all legitimate communications to flow freely.

An antivirus is a program that detects an infection and takes steps to eliminate it: it disinfects or deletes infected files. Antivirus software also works as a preventive measure. It not only fights, but also prevents your computer from becoming infected in the future. Antivirus software allows a business to protect itself from spyware, malware, phishing attacks, spam attacks and other cyber threats. DLP is a set of tools and processes that are used to prevent the loss and misuse of sensitive data.

The DLP system monitors all traffic on a secure corporate network and allows you to detect policy violations, unauthorized access to data by unauthorized users, and block attempts at unauthorized transfer of critical corporate data.

The main line of defense for corporate email is a secure gateway. It filters malicious messages and quarantines them. The secure email gateway can block up to 99.99% of spam and detect and delete emails containing malicious links or attachments.

SIEM systems collect and integrate data from the entire IT infrastructure: from host systems and applications to security devices. Afterwards, the classification and analysis of incidents and events occurs. SIEM systems, based on the correlation rules of received events, identify potential information security incidents and notify the security administrator about this.

Organizational measures include regular in-house webinars and training in the basics of digital security. This helps increase employee awareness and ensure they have the skills needed to detect and counter attacks.

Full access of each employee to all company data has its own risks - leakage of client databases, insider trading and disclosure of information about innovative activities. Companies need to clearly delineate user access rights to corporate systems, files and equipment.

An information security audit of an IT infrastructure is an independent assessment of the company’s security level for compliance with recognized practices in the field of digital security, as well as legal requirements: international standard ISO/IEC 27001, Federal Law-152 “On Personal Data” and Federal Law-187 “On Security” critical information infrastructure."

The audit includes an assessment of the effectiveness and reliability of existing protection methods, an analysis of weaknesses and vulnerabilities, as well as an assessment of their criticality and the development of recommendations for their elimination.

A digital security audit is the most important measure when developing a concept for protecting the IT landscape. However, it is only truly effective if it is carried out at regular intervals and not as a one-time initiative.

In addition to the audit, it is worth paying attention to penetration testing - PenTest. This is an imitation of a real attack using techniques and methods that attackers use to identify vulnerabilities in a company’s IT infrastructure.

Conducting PenTest allows a business to get a real assessment and a complete picture of the level of security of the infrastructure and all information systems, as well as create a list of actions and measures necessary to improve the level of security.

INFORMATION WARS AND SECURITY

The main goal of information warfare is to ensure the national security of the country, when it is necessary to solve the problems of influencing the opposing side and protecting one’s own information resource and related systems.

This version of the conceptual foundations of information warfare is based on its intermediate status between the “cold” war, which includes an economic one, and the “hot” war with its real hostilities.

Information warfare presupposes mastery of situations.

Cognitive war, that is, the war of knowledge and meaning, obviously does not boil down to information attacks. One of the key areas of modern cognitive warfare is the introduction of new educational standards and technologies.

The loss of the national education system is no less dangerous than defeat on the information front.

The centers for organizing cognitive warfare in the hierarchy of world global governance are located above the centers of information warfare, because their subject is the strategy of global development, while the main task of the media becomes information and communication services for the interests of these centers.

Cognitive hacking aims to manipulate the user's perceptions so that an attack can be carried out.

Cognitive warfare can hide unnoticed in a television series, novel, or song. It is encoded in words and people. The technology's originator is François du Clusel, a former French military officer who helped create the NATO Innovation Hub (iHub) in 2013. The center is located at Norfolk Air Base, Virginia. iHub receives funding from the Allied Command Transformation (ACT), which is one of two strategic commands at the head of NATO's military command structure. The essence of technology is a systematic impact on people’s consciousness and their way of thinking.

According to the new NATO concept, the task of cognitive warfare is “personality hacking” by using “vulnerabilities of the human brain” for the subsequent use of “social engineering” in order to reformat a person.

Within the network, even advertising is involved in systemic influence. Through it, the interests of a particular person are tracked. The massive collection of data by Western intelligence agencies was confirmed by Evadr Snowden, a former CIA employee, who disclosed information about the intelligence services' program for tracking Americans and foreign citizens through telephone and the Internet - PRISM.

In the long term (from one to several decades) this is a reboot of historical self-awareness, the education and upbringing system, the basic meanings and goals of society Including the rewriting of history, the destruction of traditions, ways of life, faith (religion) and basic values. In the medium term - the implementation of the impact on norms of behavior, undermining trust in government, splitting society.

In the long term (from one to several decades) this is a reboot of historical self-awareness, the education and upbringing system, the basic meanings and goals of society. In the medium term - the implementation of the impact on norms of behavior, undermining trust in government, splitting society.

Both technologies use informational and psycho-emotional components. The information component involves changing the content of knowledge, facts and information. That is, misinformation, substitution of concepts. The objects of influence are: news, analytical and sociological data, training programs in higher educational institutions and schools.

The psycho-emotional component uses the manipulation of consciousness, moods and emotions, when the necessary moods, assessments, opinions about something or someone are indirectly introduced to an individual, groups of people and society as a whole, and all this is accepted by people unconsciously, without understanding the essence. Cognitive warfare has swallowed up information warfare.

EXISTENTIAL THREATS

An existential threat is a danger that can seriously jeopardize the existence and development of any entity, be it an individual, a community, or even the entire human race. The impact of an existential threat can be multiple and span many different areas of life.

One of the main effects that an existential threat can have on one's existence is the loss of meaning in life. When a person or community is faced with a threat that calls into question their existence and future, they begin to question whether life has meaning. Decreased motivation, apathy, depression - all these phenomena can be a consequence of an existential threat.

In addition, an existential threat can have an impact on the psychological state of an individual or community. Feelings of constant danger and fear can cause anxiety, nervousness and increased tension. In this state, the psyche of a person or group of people may not be able to function effectively, which leads to a deterioration in living conditions and quality of life.

Also, an existential threat can lead to social discord and conflict. When people feel in danger and fear for their lives, they may become aggressive and cruel towards other people. An existential threat can divide society into groups, creating confrontation, hostility and misunderstanding.

Another impact of existential threat on existence is a change in values and priorities. When life itself is threatened, people begin to reassess their values and guidelines. Material wealth and individual achievements may give way to love, family, spiritual and moral values.

In general, the existential threat has a serious impact on the existence and development of humanity. It can cause loss of meaning in life, anxiety, social discord and changes in values.

Therefore, it is important to take all possible measures to prevent and eliminate such threats in order to ensure the stability and well-being of our modern civilization.

THREAT TO THE EXISTENCE AND DEVELOPMENT OF HUMANITY

Currently, humanity is facing a number of existential threats that can cause serious harm to its existence and development. These threats are global and pervasive, and their consequences can be long-lasting and catastrophic.

One of the main threats is climate change. The increase in temperature on Earth as a result of greenhouse gas emissions into the atmosphere leads to global warming. This causes a variety of consequences, such as changing weather conditions, rising sea and ocean levels, droughts and floods.

All this negatively affects natural ecosystems and leads to loss of biodiversity, which can ultimately lead to irreversible destruction of ecosystems and a reduction in the planet's resources. Another serious threat is nuclear war. The presence of nuclear weapons in many countries of the world creates a real possibility of their use. A nuclear conflict could lead to mass destruction and loss of life, including a very likely “nuclear winter” that could potentially cause climate change and planet-wide famine.

Information technology and artificial intelligence also pose threats to humanity. Modern technologies can be used to create cyber attacks, manipulate information and control society. The development of artificial intelligence could create a situation where machines become smarter and more powerful than humans, potentially threatening the existence of humanity.

Finally, global epidemics and pandemics are other threats to humanity. Outbreaks of new and dangerous infectious diseases can spread across the planet, causing significant loss of life and impacting public health and the economy.

To counter these threats, global cooperation and collective action must be developed. Strengthened international coordination and cooperation can help prevent and manage existential threats, ensuring the survival and well-being of all humanity.

EXISTENTIAL THREAT: THE IMPORTANCE OF PREVENTION

An existential threat is a danger that can lead to the destruction of humanity or serious damage to its existence and development. It includes various types of threats such as nuclear war, global warming, pandemics, artificial intelligence, space disasters and others.

Preventing an existential threat is essential to ensuring the safety and well-being of humanity. The goal of prevention is to take action and develop strategies that will avoid the occurrence of a threat or minimize its impact if it does occur. The importance of preventing an existential threat is as followsю. Prevents is an existential threat allows us to save people's lives and provide them with the necessary conditions for development and prosperity.

Preservation of civilization and culture: Preventing threats helps preserve the values and achievements of human civilization, as well as preserve the cultural heritage of generations. Preventing an existential threat helps preserve natural resources and biodiversity, ensuring the sustainable development of the planet. Security of the global community: Preventing a threat helps ensure the security of all countries and peoples, since the negative consequences of an existential threat can spread globally.

To effectively prevent an existential threat, the joint effort and cooperation of all participants in the international community is necessary. It is important to develop and implement international strategies and policies, as well as research and development in science, technology and innovation, to detect and analyze potential threats, develop effective prevention measures and respond to emerging threats quickly and effectively.

Thus, preventing an existential threat is an integral part of the security of humanity and its future development. It requires joint efforts and long-term strategies to ensure the preservation of life, the preservation of civilization and culture, the protection of nature and the provision of security at the global level.

THE ROLE OF SCIENCE IN DETECTING AND ADDRESSING THREATS

Science plays a key role in identifying and solving existential threats that pose a threat to the existence and development of humanity. Using the scientific method, researchers discover and analyze different types of threats to develop effective strategies and solutions to prevent or mitigate them.

One of the key aspects of science's role in threat detection is data research and analysis. Scientists collect and analyze information about various aspects of existential threats, including their nature, likelihood of occurrence, and potential consequences. This data allows you to better understand threats and determine measures to overcome them.

Scientific methodology also makes a significant contribution to establishing cause-and-effect relationships between various factors and threats. Research can identify factors that contribute to the emergence of threats, as well as predict their potential development in the future. Based on this information, appropriate strategies and actions can be developed to prevent or reduce threats.

Additionally, science plays a critical role in developing new technologies and innovations that can be used to detect and address threats. Engineers, technologists, and others are working to develop new threat detection and resolution tools, such as early warning systems, intelligent analytics tools, and more. These technologies help detect and analyze threats more efficiently and quickly, leading to more effective threat resolution.

Additionally, science plays an important role in education and public awareness of existential threats. Scientists, communicators and journalists serve as educators and informants, helping people better understand and understand the threats facing humanity and encouraging them to take necessary action to prevent them and reduce risks.

Overall, science is a key tool in detecting and addressing existential threats. Research, data analysis, technology development and education play an integral role in finding and applying solutions that will help secure the existence and development of humanity.

The main reason for the emergence of digital systems is the need to intensify problem solving and the importance of optimizing social relations associated with solving these problems.

Science is a key tool in detecting and addressing existential threats. Research, data analysis, technology development and education play an integral role in finding and applying solutions that will help secure the existence and development of humanity.

The main reason for the emergence of digital systems is the need to intensify problem solving and the importance of optimizing social relations associated with solving these problems. A prerequisite for the creation of digital systems is the redundant capability of digital systems, which can be provided in one form or another to solve third-party problems.

DIGITAL PLATFORMS

A platform is a platform that provides opportunities for others. One of the key functions of the platform is to provide commercial, communication, marketing, and investment opportunities to two or more categories of market entities. Unlike a closed ecosystem (self-sufficient and self-improving), the platform is a resource and opportunity for non-resident users.

Online platform – a digital "window of opportunity" service that facilitates interaction between two or more separate but interdependent users (whether firms or individuals) who interact through the service via the Internet

The platform, thanks to its communicative, technical, technological, organizational, and marketing capabilities, contributes to: communications (social functions), scientific development, implementation of ideas (scientific platform), better finding, searching, informing (communicative), promotion and popularization (marketing) earnings (economic).

An online trading platform is just a special case of digital platforms. There are fintech platforms, innovation development platforms, startup platforms, educational platforms.

Marketplace is a highly specialized digital platform that offers various seamlessly integrated or naturally complementary products and services that cover the widest possible range of needs of one customer profile.

DIGITAL ECOSYSTEMS

This is true for natural, man-made or digital systems. People, as well as the complex of various digital mobile and digital stationary devices they use, as well as digital devices in the real world, the developed capabilities and mutually integrated services they provide, form a digital ecosystem. First of all, when they talk about ecosystems, they mean:

Closed systems (self-sufficient, sustainable and self-improving), in which a microclimate is created that promotes the development of everything in the system. The purpose of everything that forms the system is twofold: to jointly improve the ecosystem and to extract personal, group and collective benefits that do not contradict the development of the ecosystem.

People use digital applications to order groceries home, and immediately pay for the purchased goods in the bank’s application, creating a benefit for those who organize such services. They register for an airline flight on the Internet, and receive tickets or confirm registration for the flight in a stationary digital airport terminal, thereby taking on some of the functions of the unified system, which simplifies the work of the service organizers.

You can register a company on the Digital Government digital service, where you can also use hundreds of other services. He makes relationships logical and simplifies processes. Access to the history of relationships with the buyer can be obtained through the CRM mobile application, where you can track the stages of working out the current contract and receive a forecast of payments in the case of regular and long-term relationships.

An ecosystem is an environment for interacting participants: organizations, project teams and individuals participating in the creation of “values” and in the development of the ecosystem itself, directly or indirectly sharing material and (or) digital resources, things and services that are somehow connected between a standardized platform.

The “architecture” of the digital ecosystem is: server infrastructure: computing devices, virtual servers, programs and algorithms, storage resources, a team of developers and engineers, management and customer services; client infrastructure: access device with sensors and user interface; data banks, algorithms for working with data.

Digital Architecture is a digital environment, the elements of which are participants (residents) and many digital services that perform tasks at different levels, access to which is carried out by the resident under a single account.

ECOSYSTEM MARKETING

The goals of companies must also undergo changes - profit maximization should no longer be considered an end in itself, profit acts as a means for development. The main goals of the company are to benefit from the development of society and maximally satisfy its needs. Moreover, these goals will be implemented in parallel, without one prevailing over the other.

The digital ecosystem helps: consumers - to navigate the digital world and support at all stages of its life cycle, companies - to benefit without destroying society and relationships in it and from the synergy of those striving for the preservation and development of other participants in the market process; the market – to develop progressively, preventing the destructive steps of individual participants in the market process; society - to build harmonious relationships aimed at the benefit of everyone.

People are at the center of the marketing ecosystem. Identified needs allow us to create digital services and products that help and provide the existing needs of consumers: food, transportation, accommodation, health, work and entertainment. However, behind each such service is the creation of a new business, the marketing of this business, integrated into the marketing ecosystem.

At the center of the infrastructure of the digital ecosystem is a digital banking service that collects the main flow of users, finances and studies the interests of users, producers of goods and financial institutions.

The digital ecosystem serves several market segments, provides end-to-end access to information and round-the-clock service - this is a new marketing paradigm. Traditionally, marketing has viewed customers, competitors, and business partners within the boundaries of a single industry and market segment.

However, market trends follow digital transformation and human mobility: new habits and types of consumption, new digital products and digital communication tools - all this requires a different approach to market activity - marketing digital mobile ecosystems. Market changes lead to changes in the organizational structure of companies - companies will become predominantly decentralized. The number of hierarchical levels will be reduced to a minimum, and teams and working groups will take the place of divisions and departments.

Features of digital ecosystem marketing competition not in the market

− segment, but for the human consumer, no matter what segment he is in;

− profit is not from the company’s capabilities and not from any of the company’s traditional activities, but profit from relationships with consumers;

− relationship marketing is not about winning the consumer over to your side, but following the person to those market segments where he is a consumer;

– the consequence of this is not the pursuit of profitability of transactions with a specific consumer, but an increase in the number of sales to this consumer, falling into different market niches and segments;

– analysis of user base data, rather than marketing activity, is the source of knowledge about consumers;

– targeted offers of goods and services from different market segments, formulated to the consumer within the ecosystem, reduce acquisition costs;

– ecosystem-wide principles for promoting ideas and products among consumers; intra-system incentives for consumers to use all platform services;

– brand is a real asset and strength of digital ecosystems.

Now ecosystems are one of the trends in the development of the high-tech business landscape. For now, they primarily work in high-tech companies, the banking sector, trading and telecommunications environments. However, the prospects in this area are enormous. These are development companies, tour operators, airlines, retail chains, car dealers, entertainment companies, etc.

The formation of ecosystems should radically transform economic realities. This is by no means about the priority of digital eco-comics over, say, energy. Any ecosystem develops only when everything in it is distributed proportionally and harmoniously. One thing is immutable: competence (not digital data, but the ability to apply knowledge) is becoming a separate product.

Capitalization of knowledge and information, the ability to develop and implement technologies, competitiveness, the use of new methods of marketing products, the efficiency of making and implementing market decisions are prerequisites for successful marketing of digital ecosystems.

SECURITY OF THE IT LANDSCAPE

Organization of the IT landscape The IT landscape unites all information systems of the enterprise. Its organization usually occurs in several stages: development, implementation, test, commissioning and further support. Before implementing the future IT infrastructure, the following stages are performed: analysis of the organization's business processes audit of the IT infrastructure analysis of available solutions calculation of the required budget.

The result of the IT infrastructure planning stage is an approved target architecture that meets business needs both in terms of efficiency and economics indicators. Implementation of IT infrastructure According to the approved technical specifications, the contractor begins to implement the project.

Depending on the scale of the project, you may need: selection and configuration of equipment and software, configuration of services, connection of services, creation of users, distribution into security groups, determination, configuration and installation of access rights in accordance with developed and approved regulations, installation and configuration of information security tools, configuration of necessary integrations testing creating maintenance regulations and instructions.

After implementation, technical specialists monitor the state of the IT infrastructure, carry out scheduled maintenance work with equipment and software, and also analyze feedback from all users. In the process of operating the IT infrastructure in an organization, new business processes arise over time, the organization develops, and along with this, the need arises to optimize the IT infrastructure.

Optimization means any changes in the IT infrastructure, which may be associated with the following processes:

increasing capacity in connection with the development of the organization (purchase of computers, servers, licenses);

introducing new systems, services and services into the existing infrastructure in connection with changes in business needs (CRM, ERP, document flow) implementation of information security tools in connection with changes in legislation or the emergence of new business areas (the need to ensure the safety of personal data) optimization of performance due to the increase in users and services For high-quality optimization of the IT infrastructure, it is necessary to hire employees.

And here, as in any business area, the main role will be played by the profitability of measures. Moreover, in the event of a data leak, one should take into account not only financial losses, but also image losses, which can sometimes be much more serious than financial ones.

DANGERS IN SOCIAL COMMUNICATION: CONFLICT

Conflict is an indicator of contradiction. Conflict is a natural state of the human psyche. The process of social development consists of conflicts and agreements, consent and confrontation.

The first attempts to understand the nature of social conflict belong to ancient Greek philosophers. Anaximander argued that things arise from a single material principle, leading to the separation of opposites from it. Heraclitus believed that everything in the world is born through a collision, that the only law reigning in space is war.

Thomas Aquinas developed the idea that wars are acceptable in society if they are just. Erasmus of Rotterdam pointed out that the conflict that has begun has its own logic of growth, drawing new forces into its orbit. The English philosopher Francis Bacon was the first to describe the causes of social conflicts within the country and possible ways to overcome them.

The state of the world requires effort. Hegel identified the main cause of conflicts as social polarization. Charles Darwin dedicated his theory to the problem of the struggle for existence. But the general features of conflict as a phenomenon typical of various areas of human life began to be studied only from the end of the 19th century.

At that time, works by G. Spencer, M. Weber, and L. Gumplowicz appeared. The conflict theory of K. Marx aroused great interest, the key theses of which are as follows.

1. The more unevenly scarce resources are distributed in the system, the deeper the conflict of interests between subordinate social groups of the system.

2. The more subordinate groups become aware of their interests the more likely they are to question the fairness of the distribution of scarce resources.

3. The more they doubt the fairness of the distribution of scarce resources, the more likely they are to engage in open conflict.

4. The greater the polarization, the more violent the conflict will be.

5. The more violent the conflict, the greater the structural changes in the system and the redistribution of resources as a result of the conflict.

The presented theses are also applicable to conflict in an organization, since one of the main causes of social conflict is the scarcity and uneven distribution of resources, in particular power.

A higher level of development of the organization and, consequently, a higher level of awareness by subordinates of their group interests, goals and values causes more frequent positive conflicts; increased mismatch between the interests of subordinates and management causes more violent forms of conflicts.

Georg Simmel is considered the first to define the term “sociology of conflict.” The more emotionally involved the groups are, the more acute the conflict; more “grouped” and united; the previously stronger agreement between the groups involved in the conflict; more conflict becomes an end in itself; conflicting groups are less isolated from the social structure and more, according to its participants, the conflict goes beyond individual goals and interests.

Thus, the stronger the emotion, the more likely it is to lead to violence. In interpersonal relationships, feelings caused by previous closeness, hostility or jealousy will lead to increased conflict.

At the same time, conflict promotes social integration, determines the nature of specific social formations, and strengthens the principles and norms of their organization. The severity of conflict interaction between groups leads to unity within it. Frequent but small conflicts lead to increased intra-group unity.

The severity of the conflict is also enhanced by the internal cohesion of the group participating in the conflict. Based on the theory of G. Simmel, methods for resolving conflicts based on consensus were developed.

In the modern theory of conflict (since the 60s of the 20th century), two directions have emerged, based on either the provisions of K. Marx or G. Simmel. In any organization, individuals and groups perform certain roles according to their affiliation with power structures. However, power and authority are scarce resources. There is a struggle and competition between subgroups of the organization for them.

The main source of conflict and change in an organization is the lack of power and authority. The peculiarities of the course of the conflict depend on the attitude and affiliation to power and authority of various role subgroups and individuals. The resolution of the conflict entails a redistribution of power, which legitimizes new groups of ruling and governed roles; they, in turn, begin to compete with each other again. Organizational development is a chain of repeated conflicts over power relations.

L. Coser's conflict theory examines the causes of conflict, severity, duration, and functions. L. Coser describes the process of the conflict as follows.

1. In any social system, a lack of balance, tension, and conflictual relationships are detected.

2. Many processes that are usually considered to destroy a system, under certain conditions, strengthen its integration, as well as its “adaptability” to environmental conditions.

3. L. Coser identifies causal chains that describe how conflict preserves or restores the integration of the system and its adaptability.

This series of causal dependencies looks like this.

Violation of the integration of the constituent parts of a social system leads to outbreaks of conflicts between the constituent parts, which causes temporary disintegration of the system. This makes the social structure more flexible, which in turn strengthens the system’s ability to use conflict to get rid of imbalances that threaten it in the future, and this leads to the fact that the system exhibits a higher level of adaptability to changing conditions.

L. Coser in his book “Functions of Social Conflicts” writes about the negative and positive functions of conflicts. The task is to limit negative functions and use positive ones. His analysis of these functions is considered classic. Negative functions of conflict:

- deterioration of the socio-psychological climate, decrease in discipline, productivity, even dismissals;
- inadequate perception and misunderstanding of each other by the conflicting parties;
- the idea of opponents as enemies; decreased cooperation; decreased effectiveness of cooperation;
- the emergence of a spirit of confrontation that draws in others;
- excessive involvement in the process of conflict interactions to the detriment of work;
- difficult restoration of business relationships;
- material and emotional costs to overcome it.

Positive functions of conflict:

- pushes the existing system of relations towards development, opens the way for innovation;
- plays an informational and connecting role (people get to know each other better);
- promotes the structuring of groups, the creation of an organization, and the unity of teams;
- stimulates people's activity, relieves submissiveness syndrome;
- stimulates personality development;
- in critical situations people show up better;
- relieves internal tension, giving it an outlet, a release of tension;

- diagnoses the situation and capabilities of the opponent, helps to understand the state of affairs.

The conflict can be classified according to the nature of the reasons that caused it. It is caused by the following three factors, due to:

- the labor process and poor communication;
- psychological characteristics of human relationships, that is, their likes and dislikes, cultural and ethnic differences between people, the actions of the leader;
- personal identity of group members, for example, inability to control their emotional state, aggressiveness, lack of communication, tactlessness.

Identifying the object of the conflict is an indispensable condition for analysis and its resolution. Otherwise, the conflict will either not be resolved or will arise again and again. A conflict situation is a situation in which there is and which can lead to conflict under a certain set of circumstances. A conflict situation contains the true cause of the conflict. It develops into a conflict as a result of the actions of one conflicting party to limit the opportunities for the other conflicting party to realize their interests. In order for a conflict situation to develop into a conflict, an incident is needed, a reason - a situational provocation of a conflict situation that arose as a result of a combination of circumstances and was the reason for the conflict.

Social characteristics of conflictants: belonging to a certain stratum of society, social group, profession, official position, social role, presence of authority. Psychological characteristics of conflictants: human personality traits. These features often largely determine the emergence, course, and results of a conflict.

The area of disagreement is not always easy to recognize. Each participant has his own idea of the conflict. This is what creates the ground for their clash. The reasons are hidden in the fact that each person develops his own set of attitudes, needs, interests, opinions and ideas on the basis of which he perceives and evaluates everything he encounters.

Because of this, he also has corresponding motives - aspirations, incentives to take actions aimed at realizing his attitudes and needs. Motives can be either conscious or unconscious.

Motivation determines a process that psychologists call goal formation. A goal acts as a mentally imagined result that an individual would like to achieve in a given situation. If two people have conflicting ideas about a situation, then their motives, accordingly, diverge.

When there is an area of disagreement, different ideas about the situation and at the same time unrealistic motives and goals, people begin to behave in such a way that their actions collide.

The actions of one side prevent the other side from achieving its goal, and therefore are assessed by it as hostile or incorrect. In turn, she takes responsible actions, which leads to an escalation of the conflict. It is very important to be able to avoid turning a conflict situation into a conflict.

Transfer usually occurs as a result of force, which is always associated with emotional experiences. The emotional state can begin to be maintained autonomously, transforming the conflict into a self-sustaining state.

If a conflict situation has already developed into a conflict, then first of all it is necessary to work with the emotional state of the participants in the conflict.

The main conflict-generating words in communication are:

- words expressing distrust: “you are deceiving me,” “I don’t believe you,” “you don’t understand”;
- insulting words: fool, stupid, lazy;
- words of ridicule: bespectacled, lop-eared, mumble, dystrophic, short;
- words expressing a negative attitude: “I hate you”, “I don’t want to talk to you”;
- comparison words: “like a pig”, “like a parrot”;
- must words: “you must”, “you must”;

• words of accusation: “you ruined everything”, “you are a deceiver”, “you are to blame for everything”;

• words expressing categoricalness: “always”, “never”, “everyone”, “nobody”.

The person being criticized, perceiving the words listed above, enters into a struggle for himself and tries to use the entire arsenal of defensive and justificatory means. This conflict situation may not become a conflict until an incident occurs - the person defending himself from these words will not be able to stand it (since he did not get enough sleep, he was wound up by the conflict situation on the bus). The culprit of the conflict is the one who first began to use the words conflictogens.

Actions that cause conflict may be the following:

• creating direct or indirect obstacles to the implementation of plans and intentions;

• failure of the other party to fulfill its duties and obligations;

• taking what should not belong (in the opinion of the other party);

• causing direct or indirect damage to property or reputation;

• humiliating actions;

• threats and other coercive actions;

• physical violence;

• desire for superiority, which includes the following manifestations: – condescending attitude – manifestation of superiority with a tinge of goodwill: “how can you not know this”, “don’t you understand”, “it was told to you in Russian.”

A condescending tone is a conflictogen;

– boasting – an enthusiastic story about one’s true or imaginary successes;

– categoricalness – a manifestation of excessive confidence in one’s rightness, self-confidence.

Aggression can manifest itself as a personality trait and situationally. A person with natural aggressiveness is a conflictogen in himself. Situational aggressiveness occurs as a reaction to current circumstances. This could be troubles, bad mood, well-being, as well as a response.

Objective factors are associated with the conditions of life, existence, as well as with some significant socio-psychological characteristics of an individual or social group that actually exist at a given time and cannot be changed in a short time. The presence of objective factors causing a clash of vital needs, interests, and goals makes conflict inevitable. The main thing is the form in which it will occur. The clash can end either in a complete severance of relations (the departure of one of the parties) or in the destruction of one of the parties.

Subjective factors are illusory, apparent circumstances that stimulate conflicting actions. Illusions become the causes that generate conflict and the incentives that support and strengthen it. The area of disagreement includes a cloud of subjective distortions and objective causes of the conflict. The energy of conflict is fueled from both real and imaginary sources. Everyone has illusions. If two subjects have different ideas about the same thing, then each of them thinks that the other's ideas are illusory.

It is difficult to find a situation where one of the parties is a net winner. Even if there is a gain in money or status, then against this background relation ships may be hopelessly damaged, health may deteriorate, and trust will be lost. Even if there are no such obvious losses, the losing side is unlikely to reconcile and will not dream of revenge.

In a conflict, the motivational tendency in the human soul that has a higher energy level wins. But in interpersonal and intergroup conflicts it is not so clear. The energy level of the conflictants' efforts does not always determine the outcome of the struggle in their favor. The strength of positions is determined in different social conditions. In physical conflicts – physical force; The outcome can be decided by the power of the law, the power of authority, reputation, effort, knowledge.

To choose a method of action in a conflict, what matters is not the absolute magnitude of this force, but the ratio, the balance of forces. The balance of power may change during a conflict. The dynamics of a conflict are largely determined by how the conflictants create and use the preponderance of forces in their favor. Therefore, an objective assessment of the balance of power in a conflict plays an important role.

As the conflict develops, it goes through several stages. Their duration is different, but the sequence is the same. Sometimes the state of affairs on the eve of a conflict may seem completely prosperous, and the conflict begins suddenly under the influence of a random factor.

But still there must be a hidden conflict situation. Most often at this stage there is an increase in tension in relations, there are prerequisites for conflict, certain contradictions, although they do not result in open conflict clashes. This is a potential or latent (hidden) conflict, characterized by a certain psychological state of people (there may be an emotional component, dissatisfaction with the existing state of affairs or the course of events).

Contradictions do not always develop into conflict. Only those contradictions that are perceived by potential subjects of the conflict as incompatible lead to an aggravation of tension and the emergence of strong emotional experiences. The pre-conflict stage can be divided into three phases:

a) the emergence of contradictions regarding a certain problem; growing mistrust and tension;

b) the desire to prove the legitimacy of their claims; being locked into one's own stereotypes; the emergence of prejudice and hostility in the emotional sphere;

c) destruction of interaction structures; increase in aggressiveness; formation of an “enemy image” and an attitude to fight.

The transition from mutual accusations to threats. At this stage, the conflict is easily resolved, since it is still easy for partners to treat each other constructively and can focus on cooperation. For a conflict to become real, an incident is necessary. An incident does not happen by accident. There is a limit to the tolerance of tension when the energy of irritation, slowly accumulated at the pre-conflict stage, breaks through the barrier.

An incident may occur by accident, or it may be provoked by the subject(s) of the conflict or be the result of the natural course of events. It happens that an incident is prepared and provoked by an indirect participant in the conflict who pursues his own interests.

If at least one of the conflicting parties believes that the use of force against the opponent is acceptable to achieve the goal, there is a risk of escalation of the conflict. The possibility of open conflict increases if the relationship with the opponent is not so important, but an urgent solution to the problem is required. The risk of violence increases.

There is a polarization of relations. If at the first two stages the conflict can be resolved subject to the coordination of interests, then at this stage, in order to resolve the conflict, it is necessary, first of all, that the conflicting parties want to resolve it, changing the attitude “We are enemies” to “We are partners”, “Together we will solve everything.”

Otherwise, it is useless to bring people to the negotiating table. Escalation can be continuous (a constantly increasing degree of tension in relations and the strength of blows exchanged between conflictants); wave-like (the tension in the relationship either increases or decreases).

The climax is usually expressed in some kind of “explosive” episode - one or several. It becomes clear to one or both parties that the conflict should no longer be continued. A climax is not always necessary; often the parties begin to look for a way out of the conflict earlier.

There is a limit to the tolerance of conflictants here. When the limit is exceeded, they get tired and begin to look for an opportunity to resolve differences. In a protracted conflict, the moment of climax does not come for a long time. Sometimes the conflict fades away. In other cases it leads to an even more intense climax.

At a certain stage in the development of the conflict, there comes a moment of reassessment of values, due to the balance of power and awareness of the real situation - the impossibility of achieving goals or the excessive cost of success. In this case, the conflicting parties try to look for ways of reconciliation and the intensity of the struggle, as a rule, subsides.

From this moment the process of ending the conflict actually begins, which does not exclude new aggravations. Sometimes it is advisable to calculate the cost of the conflict and the cost of exiting the conflict in order to understand that it is time to stop it.

The cost of exiting a conflict can vary greatly depending on the conditions of exit. The conflict can be stopped under the pressure of a third force, neutral or helping one of the parties. Methods for ending a conflict are aimed mainly at changing the conflict situation itself - either by influencing the participants, or by changing the characteristics of the object of the conflict.

The end of a direct confrontation between the parties does not always mean that the conflict is completely resolved. Conflict rarely goes away without leaving a trace. It leaves subjective consequences and a changed objective situation. This influence is called the aftereffect of the conflict.

If the parties believe that the agreement infringes on their interests, then tensions will continue, and the end of the conflict may be perceived as a temporary respite. Peace made as a result of exhaustion may be perceived as a temporary respite. Lasting peace can only be concluded if each side considers the conflict to be fully resolved and builds its relationship relationships based on trust and cooperation.

To reduce tension and peacefully resolve conflict relations, it is useful for the conflicting parties to reach agreement on any special rules governing the procedures for contacts between them. Conflicting parties in any sphere of human activity should use against each other only those means that are appropriate to this sphere. When the unity of norms disappears, conflict becomes especially dangerous and destructive. The problem of conflict in the context of intercultural differences is particularly difficult.

REFERENCES

1. Berry, D. (2016). The philosophy of software: Code and mediation in the digital age. London: Palgrave Macmillan. https://doi.org/10.1057/9780230306479

2. Bharadwaj, A., Sawy, O.A., Pavlou, P., Venkatraman, N. (2013). Digital business strategy: toward a next generation of insights. MIS quarterly. 2013; 37(2):471–482. URL: https://www.jstor.org/stable/43825919

3. Bikeev I. I., Kabanov P. A., Begishev I. R., Khisamova Z. I. Criminological Risks and Legal Aspects of Artificial Intelligence Implementation // In Proceedings of the International Conference on Artificial Intelligence, Information Processing and Cloud Computing (AIIPCC'19). Association for Computing Machinery. New York, USA. Article 20. Pp. 1–7. DOI: 10.1145/3371425.3371476

4. Bostrom, N. (2020). Superintelligence: Paths, Dangers, Strategies. Oxford: Oxford Univ. Press. 390 p. DOI: 10.2445/75584-1467-1444

5. Burström, T., Parida, V., Lahti, T., Wincent, J. (2021). AI-enabled business-model innovation and transformation in industrial ecosystems: A framework, model and outline for further research. Journal of Business Research; 127:85–95. https://doi.org/10.1016/j.jbusres.2021.01.016.

6. Chanias, S., Myers, M.D., Hess, T. (2019). Digital transformation strategy making in pre-digital organizations: The case of a financial services

provider. The Journal of Strategic Information Systems. 2019; 28(1):17–33. https://doi.org/10.1016/j.jsis.2018.11.003

7. Chen, D.Q., Mocker, M., Preston, D.S., Teubner, A. (2010). Information systems strategy: reconceptualization, measurement, and implications. MIS quarterly: 34(2):233–259. https://doi.org/10.2307/20721426

8. Córdova, F. (2021). Cyber-social-technological-cognitive (CSTC) approach in ecosystems: trends and challenges. 2021. IEEE International Conference on Automation/XXIV Congress of the Chilean Association of Automatic Control (ICAACCA). IEEE, 2021. P. xxxii–xxxii. https://doi.org/10.1109/ICAACCA51523.2021.9465304

9. Davtian, A., Shabalina, O., Sadovnikova, N., Parygin, D. (2021). Cyber-social system as a model of narrative management. In: Kravets A.G., Bolshakov A.A., Shcherbakov M. (eds). Society 5.0: Cyberspace for Advanced Human-Centered Society. Studies in Systems, Decision and Control, Vol. 333. Springer, Cham. P. 3–14. https://doi.org/10.1007/978-3-030-63563-3_1

10. Donnelly, N., Stapleton, L. (2021). Digital Enterprise Technologies: Do Enterprise Control and Automation Technologies Reinforce Gender Biases and Marginalisation? IFAC-PapersOnLine. 2021; 54(13):551–556. https://doi.org/10.1016/j.ifacol.2021.10.507

11. Doostmohammadian, M., Rabiee, H.R., Khan, U.A. (2019). Cyber-social systems: modeling, inference, and optimal design. IEEE Systems Journal; 14(1):73–83. https://doi.org/10.1109/JSYST.2019.2900027

12. Fredkin, E. (2003). An introduction to digital philosophy. International journal of theoretical physics; 42(2):189–247. https://doi.org/10.1023/A:1024443232206

13. Hamzaoui, M.A., Julien, N. (2022). Social Cyber-Physical Systems and Digital Twins Networks: A perspective about the future digital twin ecosystems. IFAC-Papers OnLine; 55(8):31–36. https://doi.org/10.1016/j.ifacol.2022.08.006

14. Henfridsson, O., Lind, M. (2014). Information systems strategizing, organizational sub-communities, and the emergence of a sustainability strategy.

The Journal of Strategic Information Systems; 23(1):11–28. https://doi.org/10.1016/j.jsis.2013.11.001

15. Humerick, M. (2016). Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence // Santa Clara High Technology Law Journal. 2016. Vol. 34, No. 4. Pp. 393–418. DOI: 10.5784/123462.246794-985

16. Yeow, A., Soh, C., Hansen, R. (2018). Aligning with new digital strategy: A dynamic capabilities approach. The Journal of Strategic Information Systems; 27(1):43–58. https://doi.org/10.1016/j.jsis.2017.09.001

17. Yilma, B.A., Panetto, H., Naudet, Y. (2021). Systemic formalization of Cyber-Physical-Social System (CPSS): A systematic literature review. Computers in Industry; 129:103458. https://doi.org/10.1016/j.compind.2021.103458

18. Khisamova, Z. I., Begishev, I. R. (2019). On Methods to Legal Regulation of Artificial Intelligence in the World // International Journal of Innovative Technology and Exploring Engineering. Vol. 9, No. 1. Pp. 515–520. DOI: 10.35940/ijitee.A9220.119119 EDN: PQJFKO

19. Lin, T.Y., Shi, G., Yang, Ch., Zhang, Y., Wang, J., Jia, Zh., Guo, L., Xiao, Y., Wei, Zh., Lan, Sh. (2021). Efficient container virtualizationbased digital twin simulation of smart industrial systems. Journal of cleaner production; 281:124443. https://doi.org/10.1016/j.jclepro.2020.124443

20. Loiko, A. (2022). Barrier-free space of socio-cultural activities of digital ecosystems // Experience Industries. Socio-Cultural Research Technologies (EISCRT). – 1(1) – P. 198-212. DOI: 10.34680/EISCRT-2022-1(1)-198

21. Loiko, A.I. (2022). Cognitive Artifacts of the Metuniverse // Вестник Самарского государственного технического университета. Серия «Философия» - 2022 – Т.4 - № 4 – С. 45-52. DOI: https://doi.org/10.17673/vsgtu-phil.2022.4.5

22. Loiko, A. (2023). Digital anthropology. – Minsk: BNTU. 196p. https://rep.bntu.by/handle/data/124686

23. Loiko, A.I. (2023). Design philosophy: digital technology. – Minsk: BNTU. 85p. https://rep.bntu.by/handle/data/126475

24. Loiko, A. (2023). Digital Ethics. – Minsk BNTU.86p. https://rep.bntu.by/handle/data/127399

25. Loiko, A. (2022). New industria. Digital ecosystems and Smart Society. – Lambert Academic Publishing. 145p.

26. Loiko, A. (2022). Neue Industrien. Digitale Ocosysteme and intelligente Gesellshaft. – Lambert Academic Publishing.153s. ISBN 978-620-4-63890-4.

27. Loiko, A. (2022). Nueva Industria. Ecosystemas digitales y sociedod inteligente. – Lambert Academic Publishing.145p. ISBN 978-620-4-63891-1

28. Loiko, A. (2022). Nouvelle Industrie. Ecosystemes numeriques et societe intelligente. – Lambert Academic Publishing.145p. ISBN 978-620-4-63892-8.

29. Loiko, A. (2022). Nueva Industria. Ecosystemdigital e societa intelligente. – Lambert Academic Publishing 2022. 137p. ISBN 978-620-4-63893.

30. Loiko, A. (2022). Nova industria. Ecossistemas digitais e sociedade Inteligente. – Lambert Academic Publishing 2022. 141p.

31. Loiko, A.I. (2021). Philosophy of information. – Minsk: BNTU.313 p. https://rep.bntu.by/handle/data/106983

32. Loiko, A.I. (2022). Philosophy of Mind. – Minsk: BNTU.168 p. https://rep.bntu.by/handle/data/109343

33. Loiko, A.I. (2022). Philosophy of Digital Technology. – Minsk BNTU.210 p. https://rep.bntu.by/handle/data/109830

34. Loiko, A. (2022). Philosophy of cognitive technology. – Minsk: BNTU.145p. https://rep.bntu.by/handle/data/119056

35. Loiko, A. (2023). Philosophy of digital economy. – Minsk: BNTU.126p. https://rep.bntu.by/handle/data/126236

36. Loiko, A.I. (2023). Philosophy: digital humanities. – Minsk: BNTU.145p. https://rep.bntu.by/handle/data/129771

37. Loiko, A.I. (2022). Technology of digital ecosystems // Вестник Самарского государственного технического университета. Серия «Философия» – Т.4 - №1 – С.49-56. DOI: https://doi.org/10.17673/vsgtu-phil.2022.1.7

38. Madadi, S., Hosseinzadeh Lotfi, F., Fallah Jelodar, M., Rostamy-Malkhalifeh, M. (2022). Centralized resource allocation based on energy saving and environmental pollution reduction using data envelopment analysis models // Business Informatics. Vol. 16. No. 1. P. 83–100. DOI: 10.17323/2587-814X.2022.1.83.100

39. Marabelli, M., Galliers, R.D. (2017). A reflection on information systems strategizing: the role of power and everyday practices. Information Systems Journal; 27(3):347-366. https://doi.org/10.1111/isj.12110

40. Midttun A., Khanieva M., Lia M., Wenner E. (2022). The greening of the European petroleum industry. Energy Policy; 167:112964. https://doi.org/10.1016/j.enpol.2022.112964

41. Morton, J., Amrollahi, A., Wilson, A.D. (2022). Digital strategizing: An assessing review, definition, and research agenda. The Journal of Strategic Information Systems; 31(3):101720. https://doi.org/10.1016/j.jsis.2022.101720

42. Morton, J., Wilson, A.D., Cooke, L. (2020). The digital work of strategists: Using open strategy for organizational transformation. The Journal of Strategic Information Systems; 29(2):101613. https://doi.org/10.1016/j.jsis.2020.101613

43. Ning, H., Liu, H., Ma, J., Yang, L.T., Huang, R. (2016). Cybermatics: Cyber–physical–social–thinking hyperspace based science and technology. Future generation computer systems; 56:504–522. https://doi.org/10.1016/j.future.2015.07.012

44. Pacaux-Lemoine, M.P., Trentesaux, D. (2019). Ethical risks of human-machine symbiosis in industry 4.0: insights from the human-machine cooperation approach. IFAC-PapersOnLine.; 52(19):19–24. https://doi.org/10.1016/j.ifacol.2019.12.077

45. Parker, G., Van Alstyne, M.W., Jiang, X. (2017). Platform ecosystems: How developers invert the firm. MIS Quarterly; 41(1):255–266. URL: https://aisel.aisnet.org/misq/vol41/iss1/15.

46. Pence, C.H., Ramsey, G. (2018). How to do digital philosophy of science. Philosophy of Science.; 85(5):930-941. https://doi.org/10.1086/699697

47. Ruel, H., Rowlands, H., Njoku, E. (2021). Digital business strategizing: the role of leadership and organizational learning. Competitiveness Review; 31(1):145–161. https://doi.org/10.1108/CR-11-2019-0109.

48. Sadiku, M.N.O., Tembely, M., Musa, S.M. (2018). Digital philosophy. International Journal of Advanced Research in Computer Science and Software Engineering; 8(5):27-28. https://doi.org/10.23956/ijarcsse.v8i5.607.

49. Sebastian, I.M., Ross, J.W., Beath, C., Mocker, M., Moloney, K.G., Fonstad, N.O. (2017). How big old companies navigate digital transformation. MIS Quarterly Executive; 16(3):197–213. URL: https://core.ac.uk/download/pdf/132606601.

50. Tapscott, D. (1995). The Digital Economy: Promise and Peril the Age of Networked Intelligence / D. Tapscott. - McGraw-Hill. - 342 p.